UNIVERSITÀ DEGLI STUDI DI URBINO CARLO BO

Dipartimento di Economia, Società, Politica

Corso Dottorato di Ricerca in Global Studies. Economy, Society and Law

Ciclo XXXVI

TITOLO TESI

PUBLIC AND PRIVATE IN THE DIGITAL TRANSITION OF PUBLIC ADMINISTRATION

SSD: IUS/10

Coordinatore: Ch.mo Prof. Antonello Zanfei

Supervisore: Ch.mo Prof. Matteo Gnes

Co-Supervisore: Ch.ma Prof.ssa Maria Alessandra Sandulli

Dottorando: Tommaso Cocchi

ANNO ACCADEMICO

2022-2023

PUBLIC AND PRIVATE

IN THE DIGITAL TRANSITION OF PUBLIC ADMINISTRATION

TABLE OF CONTENTS

3. Cybersecurity in the source of law system

4. Cybersecurity as award criteria: lights and shadows of the changes brought by the new Public Procurement Code.

5. Compliance with cybersecurity *standards* as a substantial market access criterion.

6. First concluding remarks

CHAPTER III

PUBLIC PROCUREMENT FOR THE PROVISION OF TECHNOLOGY SOLUTIONS. TRANSPARENCY AND COMMERCIAL SECRECY

1. Introduction

2. Public Procurement as "tool" and "purpose" of the digital transition

3. Algorithmic "opacity" between the principle of transparency, the right to good administration, trade secrets and intellectual property. Perspectives *de iure condito* in the light of the European legal context

4. Perspectives *de jure condendo* in the light of the proposed Regulation on AI

5. First concluding remarks

CHAPTER VI

Concluding remarks. The impact of technological innovation in the dialectic between public and private actors: is there an evolution of the traditional dichotomy?

BIBLIOGRAPHY

INTRODUCTION

In recent years, a number of issues have emerged that public actors need to address, such as the idea of cyberspace as a public good global, the danger of algorithm-dominated decision-making processes, as well as the damage so-called fake news and disinformation can cause to both individuals and society as a whole.

Technological advancement, defined by some as a revolution has, on the other hand, always prompted new representations of the "machina machinarum" State. To this day, the very sovereignty of States is being challenged by what has been called, with an oxymoron, the "private sovereignty" of planetary-scale enterprises. In this context, public law must prepare effective countermeasures, as it is increasingly forced to chase a very rapidly changing reality that would instead require timely reactions from national and supranational institutions.

New technologies, from the web, to 5G connections, artificial intelligence, blockchain, and the metaverse, create new market contexts, generate lifestyles, and initiate new ways of relating people and things. These are radical changes that mark an epoch in the evolution of humankind.

In this context, the public administration plays multiple "parts in the game". It, just like the community, undergoes technological evolution and is affected by it; however, it often uses it to carry out its functions; finally, it attempts to exercise the essential regulatory activity against it.

With reference to this evolutionary process, some authors have begun to speak of a "Digital State" which, while continuing to perform its traditional functions presents at least two new features compared to the past. In one respect, public activity as a whole is being transformed, both in ways and

means, through the application of new technologies. In essence, whether it is security or public services, infrastructure construction, currency, defense, health, or territorial government, the use of technological tools is required, and this phenomenon calls for the redefinition of the rules of exercise of public power and the related modes of control.

In competitor profile, technological development invests economic and social relations to such an extent that existing rules are often unsuitable and obsolete. Hence the need for new public regulation aimed at updating existing disciplines, and introducing principles and rules that adapt to such new phenomena, as is happening with digital services and the application of artificial intelligence.

Given the inescapable need for a digital transition of public administration, it has been placed at the center of investments related to the Next Generation Eu.

To live up to the needs of the community, the administration's digital transition process must inevitably materialize in its use of artificial intelligence systems, *software*, *data computing* and *blockchain* platforms. In most cases, administrations do not have in-house expertise to integrate these tools into their infrastructure, which inevitably leads them to turn to the *outsourced* market.

This trend places the dialectic between the public and private sectors, between government and large companies specializing in the implementation of high-tech solutions, at the center of the debate. Indeed, the latter are called upon to contribute to the pursuit of the public interest through the provision of suitable tools to guide the public sector's digital transition. According to some authors, there is a real relationship of subordination of the public sector to the private sector that is rooted in the inability of public administrations to

formulate their digital transformation strategies and identify the technological tools needed to implement them. Added to this is the fact that the *Information and Communication Technologies* market has been characterized by very strong concentration and is now dominated by a few multinational players. These circumstances, in essence, place government and international *big tech* in a state of mutual interdependence. Indeed, on the one hand, big companies base an increasingly large part of their *business* on institutional orders; on the other hand, we repeat, the digital transition process of public administrations would be difficult, if not impossible, without the contribution of private technology partners.

In this context, where we move in the direction of a *Governement as a Platform* model in the face of the significant benefits that may be generated in terms of growth, there will also arise for governments (and for administrative law scholars) the need to think about a resilient regulatory framework, capable of adapting to the speed of change produced by the digital transition.

The purpose of this dissertation is to analyse the evolution of the dialectic between public and private actors in the context of the digital transition of the public sector.

To pursue this objective, I have decided to divide the work essentially into three parts.

In the first part, an attempt will be made to outline the context of the digital transition of public administration, highlighting the relevant legal framework and the main actors in the European system.

The second part, on the other hand, will look specifically at two areas in which the relationship between public and private actors is evolving strongly. The first area is that of cybersecurity of public digital infrastructures. The

second, on the other hand, is the procurement of software by public actors and the related issue of transparency of the source code. In both of these areas, an attempt will be made to highlight the essential role played by private economic operators and the difficult balance between the search for efficiency and the maintenance of fundamental guarantees, both for the companies providing technological solutions to public administrations and for the citizens receiving the public services provided through these technological solutions.

In this context one is always moving, as we shall see, on rather slippery ground. On the one hand, indeed, one cannot risk "disincentivising" big tech to contribute to the digital transition process. On the other hand, it is crucial that these companies move within a precise regulatory framework, to avoid their power becoming even stronger than the public one.

In the third and final part of the dissertation, an attempt will be made to draw the threads of the dissertation, highlighting the points of arrival achieved and the way ahead.

CHAPTER I

ON THE PROCESS OF DIGITIZATION OF PUBLIC ADMINISTRATION

SUMMARY: 1. Public administration in the era of digital transition. 2. Digitization of public administration in the source of law system: a multilevel approach. 3. The players of the digital transition. 4. The effects of digitization on the organization of public administration: digitization and public procurement in the light of the new Code. 5. The effects of digitization on the actvity of public administration: participation, automation and principles of algorithmic rule of law.

1. Public administration in the era of digital transition

The theme of using new technologies to serve the public sphere is not new. As early as 1979 Massimo Severo Giannini, in his *Report on the Main Problems of State Administration drew* attention to the use of technologies by the public administration as a functional tool for improving the services offered[1] . This led to the peaceful recognition on the part of administrations of the possibility of using technological solutions capable of replacing all or part of human activity in the management of administrative procedures[2] .

This phenomenon, moreover, has been gradually developing in one with the galloping technological progress that has been characterized by considerable acceleration in recent years. With specific reference to artificial intelligence, there has been the evolution of sophisticated systems capable of collecting, reprocessing and comparing an unimaginable amount of data, as well as suggesting organizational solutions or making decisions. This has inevitably begun to reverberate on the work of public administration, leading

[1] *Report on the main problems of the State Administration* presented to Parliament on November 16, 1979 by then Minister of Public Service M.S. Giannini. Reference taken up in A. POLICE, *Scelta discrezionale e decisione algoritmica*, in *Il diritto nell'era digitale*, edited by GIORDANO, PANZAROLA, POLICE, PREZIOSI, PROTO, Milan, 2022, 496. For an in-depth examination of the Report, see G. D'AURIA, *Giannini e la riforma amministrativa*, in *Riv. Trim. dir. Pubbl.,* 4, 2000, 1209.

[2] A. POLICE, *Scelta discrezionale e decisione algoritmica, cit.,* 497; as well as, for all, A. MASUCCI, *L'atto amministrativo informatico*, Naples, 1993.

some authors to use the effective expression “Public Administration 4.0”[3] , referring to a public-private dialectic characterized by an accentuated pervasiveness of new technologies to support administrative action and the delivery of public services.

In recent years, a number of issues have emerged that public actors need to address, such as the idea of cyberspace as a public good[4] global, the danger of algorithm-dominated decision-making processes, as well as the damage so-called fake news and disinformation can cause to both individuals and society as a whole. Technological advancement, dubbed by some as a revolution[5] has, on the other hand, always prompted new representations of the "machina machinarum" state[6] . To this day, the very sovereignty of states is being challenged by what has been called, with an oxymoron, the "private sovereignty" of planetary-scale enterprises[7] . In this context, public law must prepare effective countermeasures, as it is increasingly forced to chase a very rapidly changing reality that would instead require timely reactions from national and supranational institutions.

---

[3] GALETTA-CORVALAN, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in Federalismi, 3/2019, where the authors, reconstructing the path of technological development of the p.a. effectively State that "*in the 20th century, the evolution of information and communication technologies (ICTs) has shaped an asymmetric combination between three paradigms of Public Administration: Public Administration 1.0, which corresponds to the classic Public Administration model of the 19th century, characterized by the use of paper, printing, and typewriter. Public Administration 2.0, which incorporates computers, text processors, printer and fax machine. Public Administration 3.0 to which, in the 21st century, the public sector has begun to migrate through the use of the Internet, digital portals, mobile applications and social networks. Currently, however, Public Administration is already in a fourth phase of evolution. This fourth phase is related to the so-called Fourth Industrial Revolution and has as its lowest common denominator a high degree of automation and interconnectedness that is exerting a major impact on human beings themselves and their way of being, as well as on their environment of reference.*"

[4] On the concept of public good see, among all, A.M. Sandulli, *Beni pubblici,* in *Enc. dir.*,V, Milan, Giuffre`, 1959; S. Cassese, *I beni pubblici. Circolazione e tutela*, Milan, Giuffre`, 1969.

[5] L. Floridi, *La Rivoluzione dell’informazione*, Turin, Codice Edizioni, 2012.

[6] L. Casini, *Lo Stato nell'era di Google,* Milan, Mondadori, 2020, 48 and the contributions cited therein on the subject including N. Irti, *Lo Stato: machina machinarum*, in *Riv. Trim. Dir. Pubbl*., 2004, 309, which takes up the formula used in C. Schmitt, *Il Leviatano nella Dottrina dello Stato di Thomas Hobbes,* 69.

[7] M. Clarich, *Prefazione*, in A. Lalli, *La pubblica amministrazione nell’era digitale*, Turin, Giappichelli, 2022, XIV.

New technologies, from the web, to 5G connections, artificial intelligence, blockchain, and the metaverse, create new market contexts, generate lifestyles, and initiate new ways of relating people and things. These are radical changes that mark an epoch in the evolution of humankind[8] .

In this context, the public administration plays multiple "parts in the play." It, just like the community, undergoes technological evolution and is affected by it; however, it often uses it to carry out its functions; finally, it attempts to exercise the essential regulatory activity against it. [9]

With reference to this evolutionary process, some authors have begun to speak of a "Digital State"[10] which, while continuing to perform its traditional functions presents at least two new features compared to the past. In one respect, public activity as a whole is being transformed, both in ways and means, through the application of new technologies[11] . In essence, whether it

---

[8] Y.N. Harari, *Homo Deus, breve storia del futuro*, Milan, Bompiani, 2018.

[9] A. Lalli, *Introduzione*, in A. Lalli, *La pubblica amministrazione nell'era digitale,* cit., XVI.

[10] L. TORCHIA, *Lo Stato Digitale. Una Introduzione,* Bologna, Il Mulino, 2023. In the same vein, on the concept of "Public Administration 4.0" see D.U. GALETTA and J.G. CORVALAN, *Intelligenza Artificiale per una pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi*, 3/2019, where the authors, reconstructing the path of technological development of the p.a. effectively State that "*in the 20th century, the evolution of information and communication technologies (ICT) has shaped an asymmetric combination between three paradigms of Public Administration: Public Administration 1.0, which corresponds to the classic Public Administration model of the 19th century, characterized by the use of paper, printing and typewriter. Public Administration 2.0, which incorporates computers, text processors, printer and fax machine. Public Administration 3.0 to which, in the 21st century, the public sector has begun to migrate through the use of the Internet, digital portals, mobile applications and social networks. Currently, however, Public Administration is already in a fourth phase of evolution. This fourth phase is related to the so-called Fourth Industrial Revolution and has as its lowest common denominator a high degree of automation and interconnectedness that is exerting a major impact on human beings themselves and their way of being, as well as on their environment of reference.*"

[11] On the phenomenon of digitization of public administration see, *ex plurimis,* without claiming to be exhaustive, *Il diritto dell'Amministrazione Pubblica digitale*, edited by D.U. GALETTA and R.CAVALLO PERIN, Turin, Giappichelli, 2020; R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm*, 2, 2020, 305 ff; *Pubblica amministrazione e Big Data: da Torino un dibattito sull'intelligenza artificiale*, edited by R. CAVALLO PERIN, Turin, Quaderni del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino, 2021; L. TORCHIA, *Lo Stato digitale. Una Introduzione,* cit., *passim*; A. LALLI, *L'Amministrazione pubblica nell'era digitale*, Turin, Giappichelli, 2022; A. MASUCCI, *Digitalizzazione dell'amministrazione e servizi publbici "online". Lineamenti del disegno normativo*, in *Diritto Pubblico*, no. 1/2019, 124; E. CARLONI, *Algoritmi sulla carta. Politiche di digitalizzazioen e trasformazione dgitale delle amministrazioni*, in *Dir. pubbl*., 2, 2019, 363 ff; F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. Inf.*, 2/2015, 227 ff.

is security or public services, infrastructure construction, currency, defense, health, or territorial government, the use of technological tools is required, and this phenomenon calls for the redefinition of the rules of exercise of public power and the related modes of control.

In competitor profile, technological development invests economic and social relations to such an extent that existing rules are often unsuitable and obsolete. Hence the need for new public regulation aimed at updating existing disciplines, and introducing principles and rules that adapt to such new phenomena, as is happening with digital services and the application of artificial intelligence[12] .

Well, given the inescapable need for a digital transition of public administration, it has been placed at the center of investments related to the Next Generation Eu[13] . With reference to the Italian context, specifically, the National Recovery and Resilience Plan[14] dedicates a specific Mission (called M1C1 - "Digitalization Innovation and Security of PA," included in the general Mission "Digitalization, Innovation, Competitiveness, Culture and Tourism") to which about twelve billion Euros of investments are dedicated.

In particular, to overcome the crisis generated by the Covid-19 pandemic, the NRP intervened with an expansive monetary policy that focuses on digitization, ecological transition, competitiveness, human capital enhancement, and attention to the health care system. The document's

[12] L. Torchia, *Lo Stato Digitale,* cit., 19; from the normative point of view, we refer to the Draft Regulation being approved by the European Parliament and the Council, aimed at establishing harmonized rules of artificial intelligence. The text of the proposal formulated by the Commission (COM(2021) 206 final) is available at the following link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52021PC0206.

[13] https://next-generation-eu.europa.eu/index_it

[14] Available at the following link: https://www.governo.it/sites/governo.it/files/PNRR.pdf. For a legal framing of the instrument see, *ex plurimis,* M. CLARICH, *Il PNRR tra diritto europeo e nazionale: un tentativo di inquadramento giridico*, July 2021, in *Corriere Giuridico*, no. 8-9/2021, 1025 ff.

foreword states that "*among the causes of the disappointing productivity performance is the inability to seize many opportunities related to the digital revolution and (...) this delay is due both to the lack of adequate infrastructure and to the structure of the productive fabric, characterized by a prevalence of small and medium-sized enterprises, which have often been slow in adopting new technologies and moving toward higher value-added productions.*" With specific reference to public administrations, it was highlighted how unfamiliarity with new technologies also affects the public sector and that "*before the outbreak of the pandemic, 98.9 percent of public administration employees in Italy had never used agile work*," which requires administrations to use efficient tools and networks. The Plan points out that among the causes of this inefficiency would be the decline in public and private investment, which has slowed the process of modernization of public administration, in infrastructure and production chains.

In other words, there emerges an awareness that digitization has a significant, cross-cutting impact on all public administrations, influencing both their activities and organization.

The NRP also requires overcoming delays in digitization processes and territorial gaps that halt the digital transition of member states in prosuttive processes, in digital processes and in the delivery of public services. In other words, the Plan, through the digitization of public administration, requires the declination of the principle of good performance under Article 97 of the Constitution.[15] Well, the National Strategy for Digital Transition points to the modernization of infrastructure, the use of *cloud computing*, and the

[15] D. BOLOGNINO-A.CORRADO-A.STORTO, *Digitalizzazione e pubblica amministrazione*, in *Il diritto dell'era digitale*, edited by R.GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO, Milan, 2022, p. 625. On the principle of good performance see, *ex plurimis,* M.R. SPASIANO, *Il principio del buon andamento*, in *Codice dell'Azione Amministrativa*, edited by M.A. Sandulli, Milan, 2017.

strengthening of cybersecurity, all accompanied by an increase in the skills of civil servants deputed to manage this process.

These interventions are cross-cutting in nature, requiring multilevel, albeit centralized *governance of the* phenomenon from an administrative point of view[16] . In particular, the Plan assigns to the Department of Civil Service and the Ministry of Digital Transition the coordinating role of promoting homogeneity and ensuring full usability of data (as well as full accessibility to databases) and strategic control over the process of reengineering procedures according to common standards, and their implementation also at the level of peripheral administrations. The Ministry will also be responsible for developing expertise in the "definition and construction" of the necessary technologies and interoperable digital infrastructure, on the basis of which the reengineered procedures are implemented.

One of the most ambitious goals is to improve the way public administration databases are interconnected, ensuring access to services based on the "*once only"* principle, as well as reducing time and costs for the benefit of citizens and private companies interfacing with public administrations. Specifically, the PNRR pursues full interoperability of public administration databases. On this point, Article 50 of the Digital Administration Code stipulates that the data of public Administrations must be "*formed, collected stored, made available and accessible with the use of information and communication technologies*," in order to allow their use reuse by Administrations and private entities, subject to the limits of the legislation on personal data. On this point, it should be clarified that Article *50-quater* of the Digital Administration Code places the onus on Administrations that entrust

[16] D. BOLOGNINO-A.CORRADO-A.STORTO, *Digitalizzazione e pubblica amministrazione,* cit., p. 626.

services under concession to include in contracts and specifications the obligation for the concessionaire to make available to the granting Administration all data acquired in the provision of the service to users and relating to the use by users of the service.

In this regard, a national *cloud* infrastructure is being developed, to which the data held by the member public administrations (National Strategic Pole) will migrate[17] , but also a National Digital Data Platform that will make possible the interoperability of the information systems of public administrations and public service managers through the accreditation of qualified entities[18] . The Digital Platform is a technological infrastructure that makes possible the interoperability of data held by (i) public administrations; (ii) public service operators, including listed companies, in relation to services of public interest; and (iii) publicly controlled companies under Legislative Decree No. 175 of August 19, 2016, excluding listed companies[19] . The platform is managed by the Presidency of the Council of Ministers and its interoperability is made possible through the accreditation, identification and management of authorization levels of entities that can operate on the same[20] . It should be recalled that Decree Law No. 109 of December 28, 2018 (the so-called Genoa Decree) provides that the National Informatics Archive of Public Works (AINOP), which was created as a tool to monitor the state of

---

[17] G. NAPOLITANO, *Il partenariato public-privato per l'implementazione del Polo Strategico Nazionale* in *Giorn. Dir. Amm.*, 6/2021, 703-707.

[18] A. SANDULLI, *Pubblico e Privato nelle Infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513. See also Article *50-ter* of the Digital Administration Code. For a detailed numerical examination of the increase in public investment in ICT, see Report 1/2023 "*ICT Spending in the Italian PA 2022. Main trends and ongoing paths"* available at the following link: https://www.agid.gov.it/sites/default/files/repository_files/26_07_rapporto_spesa_ict_2022.pdf

[19] V. DONATIVI, *Le società a partecipazione pubblica,* Milan, 2016; *Codice delle Società a partecipazione pubblica*, edited by G. MORBIDELLI, MILAN, 2018;

[20] In compliance with privacy regulations, the data will be searchable and accessible by accredited parties through *Application Program Interfaces*, which make programs and platforms communicating

maintenance of public works in order to ensure the safety of users[21] , will also interact with this platform.

In essence, to live up to the needs of the community, the administration's digital transition process must inevitably materialize in its use of artificial intelligence systems, *software*, *data computing* and *blockchain* platforms.

For the purposes of this paper, however, it is crucial to note that in most cases, administrations do not have in-house expertise to integrate these tools into their infrastructure, which inevitably leads them to turn to the *outsourced* market[22] .

This trend places the dialectic between the public and private sectors, between government and large companies specializing in the implementation of high-tech solutions, at the center of the debate. Indeed, the latter are called upon to contribute to the pursuit of the public interest through the provision of suitable tools to guide the public sector's digital transition. According to some authors, there is a real relationship of subordination of the public sector to the private sector[23] that is rooted in the inability of public administrations to formulate their digital transformation strategies and identify the technological tools needed to implement them. Added to this is the fact that the *Information and Communication Technologies* (so-called ICT) market has been

---

[21] D. BOLOGNINO-A.CORRADO-A.STORTO, *Digitalizzazione e pubblica Amministrazione,* cit. p. 637; D. BOLOGNINO,*Il c.d. Decreto "Genova": tra intervento per la salvaguardia e la ripresa economica della città e l'implementazione sistemica della sicurezza per le infrastrutture nazionali,* LUISS Guido Carli University, November 29, 2019, in Amministrazione in cammino, November 12, 2020.

[22] D.U. GALETTA, *Transizione digitale e diritto ad una buona amministrazione*, cit., 109 as well as the contribution cited therein Mary C. Lacity-Rudy Hirschheim, *Information systems outsourcing; Myths, Metaphors and Reliabilities*, John Wiley & Sons Ltd, England, 1993.

[23] A. NATALINI, *Come il passato influenza la digitalizzazione della pubblica Amministrazione*, in *Riv. trim. dir. pubbl.,* no. 1, 2022, 95; A. SANDULLI, *Pubblico e privato nelle infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl*., 2021, 513.

characterized by very high concentration and is now dominated by a few multinational players[24] .

These circumstances, in essence, place public administrations and international *big tech* in a state of mutual interdependence. On the one hand, in fact, big companies base an increasingly large part of their *business* on institutional orders; on the other hand, it is repeated, the digital transition process of public administrations would be hardly feasible, if not impossible, without the contribution of private technology partners[25] .

Ultimately, it should be noted that digital administration, therefore, is both an engine for the country's development and the enhancement of opportunities for its citizens and businesses but also a crucial goal to pursue, the achievement of which requires the adoption of structural measures to achieve ever-increasing connectivity, social inclusion and cohesion of society, and effective governance of the implementation process[26] .

In this context, scholars of administrative law are called upon to reason about whether, and in what terms, the Administration's use of AI can be a suitable factor in the pursuit of the public interest, without, however, losing sight of the "traditional" categories of administrative science. Indeed, one can, as proposed by some Authors, think of an "updating"[27] of some classical theorizations of administrative law, but the coordinates, both for the legislator

---

[24] On this topic, see L. CASINI, *Lo Stato nell'era di Google*, in *Riv. Trim. Dir. Pubbl.*, 2019, 1125, where the author highlights The different aspects of the influence of big companies (especially the tech sector) on democratic systems. On the topic see also, M.R. FERRARESE, *Poteri nuovi,* Bologna, Il Mulino, 2023.

[25] For a reconstruction of the new ordinamental arrangements in this area see O. POLLICINO, *Digital Power*, in *Encyclopedia of Law*, *Thematics*, V - 2023, 410 ff., where the author speaks of the "transfiguration" of private subjects from economic actors to powers in the strict sense.

[26] B. MARCHETTI, Voce *Amministrazione Digitale,* in *Enciclopedia del Diritto*, Milan, 2022, 76.

[27] GALETTA-CORVALAN, *Intelligenza artificiale per una pubblica Amministrazione 4.0?*, cit., 7 as well as TORCHIA, *Lo Stato digitale. Una introduzione,* Bologna, 2023, 110, according to which "*a comprehensive reconsideration of some fundamental principles and institutes of administrative law is required (...): from the principle of legality to the rules for the conduct of administrative proceedings, from the exercise of discretionary power to the judicial review of that power.*"

and the Administration, must be clear in order to avoid irreparable compression of the positions of the administered. Indeed, it cannot be admitted that algorithmic administrative power is not governed by the same principles and is not subject to the same constraints and conditions as "traditional" administrative power[28] .

2. Digitization of public administration in the source of law system: a multilevel approach

The increasing integration of Italian law with supranational law has led to a proliferation of sources with which interpreters and practitioners have to deal[29] .

For this reason, it is customary to speak of a "*multi-level protection* system"[30] which on the one hand has led to greater guarantees and protections for citizens, and on the other has increased the task of the jurist called upon to apply the rules.

In order to better understand the complex relationship between the domestic and supranational legal systems, it is worth recalling the concepts of dualism and monism - obviously referring to the legal system - as theorised by Hans Kelsen. Indeed, according to the philosopher, following a monist approach "*the two sets of apparently different norms can constitute a*

---

[28] TORCHIA, *Lo Stato digitale. An Introduction,* Bologna, 2023, 110, where it is argued that "*if this sort of 'exemption' were to be realized, in fact, we would be faced with a sort of regression - anti-historical and even unconstitutional - to the regime of tendential immunity that in a past no longer recent characterized public power.*"

[29] On the poin see F. FRANCARIO - M.A. SANDULLI, *Principio di ragionevolezza delle decisioni giurisdizionali e diritto alla sicurezza giurdica,* Editoriale Scientifica, Naples, 2018; M.A. SANDULLI, *I Principi costituzionali e comunitari di giurisdizione amministrativa,* in *Il nuovo processo amministrativo,* edited by M.A. SANDULLI, Giuffrè Editore, Milan, 2013, p. 29.

[30] For an in-depth analysis see M. CARTABIA, *La tutela multilvello dei diritti fondamentali. Il cammino della giurisprudenza della Corte Costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona*, in cortecostituzionale.it, 2014; F. PATRONI GRIFFI, *La giustizia Costituzionale in trasformazione: La Corte Costituzionale tra Giudice dei diritti e Giudice dei conflitti,* in Federalismi.it.

unitary system either because one system can find in the other the basis of its validity, or through an *equalization between the two* systems".[31]. According to some scholars[32], the dualist approach has had a profound effect on the relations between the Italian and European legal systems; the production of legal effects by the supranational system in the domestic one depends on the Italian state opening up to the European system[33] , through a voluntary absorption of rules, precepts and values to which, moreover, a superordinate position is recognized, precisely because of the recognition as an autonomous and separate legal system.

This phenomenon is particularly pronounced with reference to the regulation of technological innovation, in which the European legislature has also taken the lead globally.

It should be premised that although the Treaties do not contain special provisions for information and communication technologies, the EU can nevertheless undertake relevant actions under sectoral and horizontal policies, such as: industrial policy (Article 173 of the Treaty on the Functioning of the European Union (TFEU)); competition policy (Articles 101-109 TFEU); trade policy (Articles 206 and 207 TFEU); trans-European networks (TENs) (Articles 170-172 TFEU); research and technological development and space (Articles 179 and 190 TFEU); and energy policy (Article 194 TFEU); the approximation of laws to improve the establishment and functioning of the internal market (Article 114 TFEU); the free movement of goods (Articles 26

---

[31] H. KELSEN, *Lineamenti di dottrina pura del diritto,* Piccola Biblioteca Einaudi, Turin, 1952, p. 155.

[32] G. PALMISANO, *Il Sistema giuridico internazionale e l'ordinamento comunitario, 2012,* in *treccani.it*.

[33] On the subject see, ex plurimis, W.V. GERVEN, *The European Union a polity of States and Peoples,* Stanford University Press, California, 2005, p.7 et seq.; A.M. CALAMIA - V. VIGIAK, *Diritto dell'Unione Europea,* Giuffrè, Milano, 2018, p.5 et seq.; G.TESAURO, *Diritto dell'Unione Europea,* Cedam, Padova, 2012, p.1 et seq.; L. NELVILLE BROWN - T. KENNEDY, *The Court of Justice of the European Communities,* Sweet and Maxwell, London, 2000, p.2 et seq..

and 28-37 TFEU); the free movement of persons, services and capital (Articles 45 and 66 TFEU); education, vocational training, youth and sports (Articles 165 and 166 TFEU); and culture (Article 167 TFEU)[34]. The necessity of a European intervention is founded both on legal factors and on opportunity. With reference to the latter, as mentioned above, it would be unthinkable to believe that it would be possible to effectively regulate such a disruptive phenomenon as artificial intelligence exclusively through the national legislation of individual Member States. Such an approach besides being completely ineffective, would provide an unacceptable "patchwork" protection of rights in the European context.

The Union should also regulate this phenomenon for legal reasons.

Firstly, the subject of technological development falls within the shared competences regulated by Article 4, par. 3, TFEU. For this reason, in the area of the development and regulation of the artificial intelligence phenomenon, the Union can legislate, as well as "*define and and implement programs*". Moreover, it must be stressed that the Union's competence is linked to the suitability of the new technologies to affect the fundamental rights protected by the Treaties (the right to human dignity, respect for private life and protection of personal data, non discrimination and equality between women and men, rights to freedom of expression, the right to an effective remedy and to a fair trial, the rights of defense and the presumption of innocence and the principle of good administration).

In addition, the regulation of the phenomenon in question, by laying down precise provisions for the implementation and development of new technologies, is inextricably linked to the regulation of the internal market,

[34] https://www.europarl.europa.eu/factsheets/it/sheet/64/l-agenda-digitale-europea.

which is another area of shared competence between the Member States and the Union.

Given the EU's competence to create an appropriate legal framework for regulating the new technologies, the first steps taken at European level should now be analyzed.

The Digital Agenda for Europe[35] , a follow-up to the Lisbon Strategy, first established the key role of new technologies in achieving European goals. In 2015, the Digital Single Market Strategy[36] further developed the Digital Agenda, establishing specific provisions based on three pillars aimed at ensuring a fair, open and secure digital environment: 1) improving consumer and business access to digital goods and services across Europe, 2) creating an enabling environment for digital networks and services to flourish, and 3) maximizing the growth potential of the digital economy.

The intent of the European legislator was to improve access to digital goods and services for consumers and businesses across Europe by equipping the EU with an advanced system of user rights and consumer and business protection, including: i) lower prices for electronic communications (Regulation (EU) no. 2022/612)[37] and the end of roaming tariffs as of June 14, 2017; ii) better Internet connectivity for all through full coverage with basic broadband, particularly through mobile and satellite broadband developments, in order to develop Gigabit connectivity for all key socio-economic actors (iii) better consumer protection in telecommunications through legislation on

[35] https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX:52010DC0245.
[36] EUR-Lex - 52015DC0192 - EN - EUR-Lex (europa.eu).
[37] Regulation - 2022/612 - EN - EUR-Lex (europa.eu).

privacy (Directive 2009/136/EC)[38] and data protection (Regulation (EU) 2016/679[39] and Directive (EU) 2016/680[40]).

The strategy, in essence, aimed to maximize the growth potential of the digital economy by promoting digital skills and high-performance computing, digitizing industry and services, developing artificial intelligence (AI), and modernizing public services.

In addition to the new data protection legislation, the EU has adopted a number of measures to facilitate the development of an agile data-driven economy[41] , such as (i) the Regulation on the Free Movement of Non-Personal Data (Regulation (EU) 2018/1807)[42] , which allows businesses and public administrations to store and process non-personal data wherever they choose to do so in the EU; (ii) the Regulation on Cyber Security (Regulation (EU) 2019/881, which will be returned to in Chapter no. 3)[43] , which strengthens the European Union Agency for Cybersecurity (ENISA) and establishes a framework for cybersecurity certification of products and services; and iii) the Open Data Directive (Directive (EU) 2019/1024)[44] , which establishes common standards for a European market for government-held data.

In 2020, Europe adopted its second five-year digital strategy[45] , titled "*Shaping Europe's Digital Future*," focusing on three key objectives in the digital sector: i) technology serving people, ii) an equitable and competitive economy, and iii) an open, democratic and sustainable society. In 2021, the

---

[38] Directive - 2009/136 - EN - EUR-Lex (europa.eu).
[39] EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex (europa.eu).
[40] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0067.
[41] For a reconstruction see *Il valore economico dei dati personali*, edited by F. LAVIOLA, E. CREMONA, V. PAGNANELLI, Turin, 2022.
[42] Regulation - 2018/1807 - EN - EUR-Lex (europa.eu)
[43] Regulation - 2019/881 - EN - EUR-Lex (europa.eu)
[44] Directive - 2019/1024 - EN - EUR-Lex (europa.eu).
[45] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0067.

strategy was complemented by the "*Digital Compass 2030: The European Model for the Digital Decade*," a 10-year tool that aims to translate the EU's digital ambitions for 2030 into concrete terms.

The second Digital Agenda focuses on the profound changes brought about by digital technologies, the essential role played by digital services and markets, and the EU's new ambitions in technology and geopolitics. Specifically, through a series of strategic acts, the Commission has set out the specific actions it intends to take to help create secure digital markets and services. In addition, priorities for the current decade include the development of quantum computing, a blockchain strategy and blockchain-based trade policy, anthropocentric and trustworthy artificial intelligence, semiconductors, digital sovereignty, cybersecurity, Gigabit connectivity, 5G and 6G, European data spaces and infrastructures, and the definition of global technology standards.

Against this backdrop, on March 9, 2021, the EU proposed a Digital Compass (COM/2021/0118)[46] , which includes four digital goals to be achieved by 2030: (i) skills (at least 80 % of adults should have basic digital skills and there should be 20 million specialists employed in ICT in the EU, with an increase in the number of women); (ii) businesses (75 % of businesses should use cloud computing, big data and artificial intelligence services; more than 90 % of small and medium-sized enterprises in the EU should achieve at least a basic level of digital intensity; the number of "unicorn" enterprises in Europe should double); iii) infrastructure (all European households should be covered by a Gigabit network and all areas inhabited by 5G cutting-edge, sustainable semiconductor production in Europe should account for 20 percent

[46] EUR-Lex - 52021DC0118 - EN - EUR-Lex (europa.eu).

of the value of global production; 10,000 climate-neutral and highly secure peripheral nodes should be installed in the EU; and Europe should have its first quantum computer); iv) public services (all major public services should be available online; all citizens will have access to their electronic health records and 80 percent of citizens should use an electronic identity solution).

In implementation of these programmatic goals, a range of funding has been allocated (in addition to the Next Generation EU mentioned above) such as the "Digital Europe" Program[47] , aimed at the development of digital technology with a planned total budget of €7.5 billion for the period 2021-2027, which will provide strategic funding to support projects in the areas of high-performance computing, artificial intelligence, cybersecurity, advanced digital skills and ensuring the broad use of digital technologies throughout the economy and society, including through digital innovation hubs.

As outlined in the White Paper on Artificial Intelligence published in February 2020, AI is believed to play a central role and is expected to bring multiple social and economic benefits to a wide range of sectors.

In this regard, on April 21, 2021, the European Commission published its proposal for a new law on artificial intelligence (COM(2021)0206)[48] , which enshrines in EU law a technology-neutral definition of AI systems and adopts a different set of standards adapted to a risk-based approach.

A further crucial step in the European strategy on the regulation of artificial intelligence was taken on April 21 last19 with the presentation (by the European Commission to Parliament) of the "*proposal for a regulation*

[47] The Digital Europe program | Shaping Europe's digital future.
[48] EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu).

laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) "20.

The document will certainly be amended, supplemented and reworked. However, it represents the first concrete attempt to regulate the phenomenon of artificial intelligence. The intention of this paper is not to analyze the detailed discipline proposed by the Commission, but to highlight the principal coordinates of the act in order to be able to reason on its exhaustiveness.

Firstly, it must be pointed out that the specific objectives of the proposal are "*i) to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; ii) ensure legal certainty to facilitate investment and innovation in AI; iii) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; iv) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation*."

In other words, the aim is to enable the sustainable development of new technologies that respect people's fundamental rights, while stimulating the development of these technologies and enabling Europe to play a strategic role in this area in a global level.

With reference to the necessity that the matter under examination is regulated at supranational level, the Commission in the introduction of the act (see Point 2.2) specifies that "*the objectives of this proposal cannot be effectively achieved by Member States alone. Furthermore, an emerging patchwork of potentially divergent national rules will hamper the seamless circulation of products and services related to AI systems across the EU and will be ineffective in ensuring the safety and protection of fundamental rights*

and Union values across the different Member States. National approaches in addressing the problems will only create additional legal uncertainty and barriers, and will slow market uptake of AI".

The scope of the regulation is very broad, covering the production, placing on the market and use of all artificial intelligence systems.

The Regulation expressly prohibits (see Art. 5) the use of artificial intelligence with the following characteristics: 1. Subliminal technologies capable of diverting the attention of individuals and confusing them; 2. AI systems that exploit the vulnerability of certain individuals or categories of individuals by affecting their ability to self-determine; 3. The use of social scoring technologies by or on behalf of public authorities; 4. The use (with some limitations) of the "real-time" remote biometric identification systems.

Particular attention of the discipline is devoted to the technologies defined as "high risk" (see Art. 6), which consist of a series of technologies able to create a risk for the health, security or fundamental rights of the persons. These technologies, in substance, are represented by the systems used as security components of some products, as well as those indicated in an annex of the regulation (where are included, among others, the systems used for personnel selection, for predictive policing).

For technologies considered to be high risk, the proposal of regulation provides for some specific rules, among which: i) the necessity that these are subject to a system of "risk management"; ii) the obligation that these systems are developed according to certain qualitative criteria relating to the management of the data; iii) the obligation of transparency toward the users regarding the functioning of these systems; iv) the obligation to guarantee the reliability and accuracy of the systems.

Compliance with these characteristics will be assessed through a detailed "conformity assessment" procedure based on particular reference standards and these products will be CE marked accordingly.

On this point, the Regulation provides for the creation of "sandboxes" aimed at experimenting with the creation and *in vitro* use of artificial intelligence systems that comply with the regulatory framework outlined. In particular, each Member State will be able to create its own "sandboxes", which will have to respect the characteristics provided for by the Regulation and on which the powers of vigilance of the competent authorities will be carried out.

In this last regard, the proposal of regulation takes a clear and distinct position on the necessity of the creation of an authority at European level (European Committee for artificial intelligence) which will have to supervise and coordinate the single national authorities. It follows, consequently, that the single Member States must create ad hoc authorities (see Art. 59 "*Designation of national competent authorities*") for the regulation of this ambit. The model, in substance, is quite similar to that relative to the protection of data, where a European central authority is flanked by the authorities of the single Member States.

The Digital Agenda also places a strong emphasis on e-government and cross-border cooperation in the public sector. On November 18, 2022, the Commission presented a proposal for legislation on an interoperable Europe, which aims to help the EU and its member states deliver better public services to citizens and businesses. The proposal calls for the creation of an Interoperable Europe Committee composed of representatives from EU member states, the Commission, the Committee of the Regions, and the European Economic and Social Committee. Among other things, the COVID-

19 pandemic has helped accelerate the development of European interoperability, as evidenced by the EU's digital COVID certificate. The proposed regulation is accompanied by a Commission communication (COM(2022)0710) aimed at raising awareness of the importance of improving cross-border interoperability and cooperation in the public sector.

Turning to the national context, the first signs of an effective pursuit of digitization of public administration in Italy can be found in the introduction within the law on administrative procedure (Law No. 241 of August 7, 1990) of Article *3-bis* (introduced only in 2005), headed "the use of telematics" under which it is established that "*in order to achieve greater efficiency in their activities, public administrations shall act by means of telematic and computer tools in their internal relations, between different administrations and between these and* private parties"[49] . In other words, a programmatic rule of general scope is inserted that requires the use of IT tools in the performance of the activities of public administrations.

The change is followed by the entry into force of the Digital Administration Code (CAD) in Legislative Decree No. 82 of March 7, 2005. The code represents the first organic discipline capable of regulating digital administration, but its continuous amendments express the difficulty of regulating a phenomenon characterized, on the one hand, by continuous and sudden technological developments and, on the other hand, by a substantial disapplication in practice, linked to the inertia of the public administration and the lack of economic resources necessary for its concrete implementation[50] .

---

[49] See F. CARDARELLI, *L'uso della telematica*, in *Codice dell'azione amministrativa* edited by M.A. SANDULLI, Milan, Giuffrè, 2017, sub art. 3-bis l. n. 241 of 1990, 519; F. COSTANTINO, *L'uso della telematica nella pubblica amministrazione*, in *L'azione amministrativa* edited by A. ROMANO, Turin, Giappichelli, 2016, 242.

[50] See B. MARCHETTI, Voce *Amministrazione Digitale*, cit. 81; E. CARLONI, *La riforma del Codice dell'AMministrazione digitale*, in Giorn. dir. amm., 2011, no. 5, 469.

The rules of the digital administration code must be read in light of the three-year plan for information technology in public administration (2020-2022) and AGID's technical standards (mostly adopted through circulars). The regulatory framework, however, does not end with these sources, since, a number of other provisions remain excluded from the code, but applicable to digital administration, which have not been incorporated into it, including d.l. Oct. 18, 2012, no. 179, which regulates the issue of public administration infrastructure and was amended both by d.l. No. 76 of 2020 and, more recently, by d.l. May 31, 2021, No. 77 21, No. 108), both aimed at ensuring the country's technological autonomy, securing the digital infrastructure of the public administration and regulating the *Cloud*, which is considered essential for the technological development of the country and the administration itself.

There are also a number of European disciplines that, as reported above, affect (and will affect) digital administration, with regard to both data and privacy protection, accessibility of services, and finally, shortly hereafter, the use of artificial intelligence, given that the proposed EU regulation on artificial intelligence adopted by the Commission in April 2021 applies as much to private producers and users of AI systems as to public administrations.

The framework of rules that in various ways concern the digitization of public administration is thus far from being unified and complete: it is the result of the combination of several regulatory levels, not only national, and is destined to be enriched and modified also due to changes and developments in technology, and must also take into account the security and *privacy* requirements that the use of digital brings with it.

With reference to the scope of application, it should be noted that the entities that are covered by the entire discipline are public administrations as per Legislative Decree No. 165 of March 30, 2001, and independent

authorities, private entities that manage public services, including listed companies as far as public interest services are concerned, and public companies (excluding listed companies, unless they fall into the previous category).

As for the supporting pillars of the legislation, according to some Authors[51] at least four main missions can be identified: the one that enunciates digital rights and lays the foundations for their concrete enjoyment, the one that establishes the organizational transformations necessary to implement digitization, the one that establishes the conditions for the validity of digital documents and communications, and the one that regulates document storage and transmission and data management, with the creation of the National Digital Data Platform.

Through the transition to digital, therefore, the smooth running of the administration must be guaranteed[52], as a result of a reorganization of the administration involving not only time savings and efficiency[53] but also a transformation of decision-making processes. Technology, in these terms, is aimed not only at speeding up existing processes, through their dematerialization, but at replacing them with digitally based and automated processes.

3. The players of the digital transition

Having completed the brief survey of the sources of digitization, it is necessary to dwell briefly on the institutional actors involved in this process. The decisive impetus given by the PNRR to the Italian digitization process has

[51] B. MARCHETTI, Voice Amministrazione Digitale, cit. 83.
[52] D.U. GALETTA, *Digitalizzazione e diritto ad una buona amministrazione*, cit., 85
[53] On digitization as a tool for administrative simplification see P. CLARIZIA, La digitalizzazione della pubblica amministrazione, in *Giorn. dir. amm.*, 2020, no. 6, 727.

produced a significant reorganization of the government's functions in the field of technological innovation. Decree Law No. 22 of March 1, 2021, assigned to the Prime Minister powers of direction and coordination in this area, for the implementation of Italy's digital agenda, for the implementation of broadband, the digitization of public administrations and businesses, the country's digital transformation, growth and transition, access to *online* services, connectivity, digital infrastructure and public data strategy.

The coordination of government action is ensured by a new Interministerial Committee for Digital Transition, which ensures the coordination of government action on ultra-wideband and electronic communication networks, health records and health data platform, and initiatives for the development and deployment of artificial intelligence, the Internet of Things (IoT) and *blockchain.* The committee also has the function of verifying the status of implementation of the digitization processes underway in the various public administrations, also in order to promote possible synergies and resolve dysfunctions and critical issues.

The support structure of the Minister for Technological Innovation and Digital Transition is the Department for Digital Transformation established by Prime Minister's Decree June 19, 2019 at the Prime Minister's Office: it has functions of promoting and coordinating government actions aimed at defining a unified strategy on digital transformation and modernization of the country.

Alongside the Department operates AGID, the agency in charge of implementing the Italian Digital Agenda (pursuant to Art. *14-bis* of the Digital Administration Code). Its functions are indicated in Art. *14-bis* of the code and consist of tasks of planning, coordinating and monitoring the activities carried out by administrative authorities for the use of digital, in the light of the objectives of the three-year plan for information technology; in the preparation,

implementation and management of innovation interventions and projects; in the promotion of digital culture and research, as well as in advising on contracts and tender procedures announced by Consip and aggregating entities for the acquisition of goods and services related to automated information systems and defined as strategic in the three-year plan.

Its action to boost the digital transition process is accompanied by supervisory and control powers over the state of implementation of the code, the three-year plan and the guidelines, to which are connected investigative powers that can be activated upon report or ex officio to ascertain any violations and consequent sanctioning powers.

It also has a fundamental regulatory function that consists in the adoption of guidelines containing rules, standards and technical guides, as well as acts of direction, supervision and control over the implementation and norms of the code, including through the adoption of general administrative acts on the digital agenda, digitization of public administration, cybersecurity interoperability and application cooperation, between public information systems and those of the European Union. On the nature of these guidelines, the Council of State ruled in 2017, on the occasion of the presentation of Legislative Decree No. 217 of 2017, recognizing the binding nature of the same and applying to them consequent procedural and procedural guarantees, according to the same logic already used with regard to the guidelines of the National Anti-Corruption Authority[54] .

In addition to the authorities directly in charge of promoting and monitoring the digitization process of public administration, the technological

[54] M. MONTEDURO, *I principi del procedimento nell'esercizio del potere sanzionatorio delle Autorità amministrative indipendenti. Tessuto delle fonti e nodi sistematici*, in ALLENA-CIMINI (ed.), *Il potere sanzionatorio delle Autorità amministrative indipendenti*, in *Il diritto dell'economia*, 2013; G. MORBIDELLI, *Il principio di legalità e i cd poteri impliciti*, in Dir. amm., 2007, 4, 703 ff.

transition also requires the creation of administrations capable of ensuring the security of the digital space or, according to a more comprehensive diction, of the environment resulting from the interaction between people, *software* and network services through technological devices. In this sense, as will be discussed *amplius* in Chapter 3, cybersecurity is a precondition of the digitization process, and it must be ensured through action against cyber threats and attacks. The establishment of the National Cybersecurity Agency that took place with Decree Law No. 82 of June 14, 2021 responds to this purpose and is part of the European cybersecurity strategy, as well as being one of the goals of the NRP.

As will be discussed in more detail in the next chapter, the Agency has personality under public law, has regulatory, organizational and financial autonomy and provides its cooperation and assistance to the Prime Minister in the field of cybersecurity. The director of the Agency and its deputy director are appointed by the Head of the Government, after notifying the President of Copasir[55] . The functions it exercises are multifaceted and range from the coordination of relevant authorities, to the functions of certification and qualification of *Cloud* services, to the supervision and monitoring of cybersecurity. It is also required to serve as the national contact point with respect to both its European counterpart Agency (European Union Agency for Cybersecurity) and in the international context.

The institutional framework is also to be enriched soon with an authority responsible for implementing the European regulation on Artificial Intelligence, as soon as the legislative process for its adoption is completed. In fact, the proposal adopted by the European Commission in April 2021

[55] Parliamentary Committee on the Security of the Republic.

envisages that member states will have an authority both for monitoring high-risk artificial intelligence systems placed on the European market and for licensing entities certifying the compliance of the same high-risk systems with the requirements set in the European framework.

4. The effects of digitization on the organization of public administration: digitization and public procurement in the light of the new Code

The described phenomenon of digitization impacts both the activity and the organization of public administration. With reference to organization for the purposes of this paper, it is useful to briefly dwell on the digitization process in the area of public contracts. The need to digitize public contracting processes, among other things, is also linked to the NRP, where a specific reform aimed at implementing an *e-platform* for public contracting is envisaged[56] .

With Legislative Decree No. 36/2023[57] it is intended to implement a new technological infrastructure that is the indispensable tool to streamline public contracting procedures and manage all administrative fulfillments affecting the different phases of public contracts. Specifically, the implementation of the National Public Contracts Database and the Virtual Dossier of the Economic Operator, with the creation of a digital infrastructure on which all the fulfillments affecting the entire lifecycle of public contracts must be managed, and the provision for the use of automated procedures constitute innovations capable of significantly affecting the market, and their implementation should

[56] P. CLARIZIA, *E-procurement*, in *The Digital State in the National Recovery and Resilience Plan*, Rome, 2022, 109 ff.

[57] Early commentators include G. CARLOTTI, *I principi nel codice dei contratti pubblici: digitalizzazione*, in giustizia-amministrativa.it, 2023, 6 and L. CARBONE, *La scommesa del codice dei contratti pubblici e il suo futuro*, in giustizia-amminsitrativa.it, 2023, 9. V. CAMPANILE, *Art. 19*, Public Contracts Code edited by C. CONTESSA - P. DEL VECCHIO, Naples, 2023.

have disruptive effects on public administrations[58] . Specifically, Through the National Public Contracts Database and telematic platforms, contracting stations are required to manage operations related to the three-year planning and programming of purchases, the initiation and publication of tender documents, the awarding process, the conclusion of the contract, and the administrative and accounting requirements necessary for the purposes of execution, up to the conclusion and testing of contracts.

The forecasts on the digitization of public contracts and, in particular, the regulations aimed at implementing the infrastructural skeleton and the national e-procurement ecosystem draw a reform that presupposes a profound reorganization, significant retraining of personnel and considerable investment in the hardware and software infrastructure of public administrations, contracting stations and economic operators in order to ensure the implementation of the new interoperable and interconnected system between the national public contracts database, the various public databases, telematic platforms and other information systems of certifying bodies and SOAs.

Principles aimed at regulating the digitization of the contract lifecycle are enucleated in Article 19 of the Code, where reference is made to the principles enucleated in the Digital Administration Code and it is stipulated that contracting stations shall operate in accordance with the principles of technological neutrality, transparency, as well as personal data protection and cybersecurity.

In the second paragraph of Article 19, the principle of once *only* is reiterated, according to which in implementation of the principle of one-time submission, each data item is provided only once to one information system,

[58] P. CLARIZIA, *Digitalizzazione,* in *Giorn. Dir. Amm.*, 3, 2023, p. 303.

cannot be requested from other systems or databases, but is made available by the receiving information system.

In the third paragraph, it is then clarified that administrative activities and processes related to the lifecycle of public contracts are carried out digitally through the digital infrastructure platforms and services of contracting stations and awarding bodies; data and information related to them are managed and made usable in an open format.

The provision also stipulates that contracting stations, as well as economic operators participating in tender activities and procedures, shall adopt technical and organizational measures to safeguard IT security and personal data protection, including ensuring adequate training of public officials. It is also specified that contracting stations and granting entities must ensure the traceability and transparency of activities carried out, accessibility of data and information, and the knowability of decision-making processes.

It should be noted that Article 19 also provides the possibility, depending on the type of procurement procedure, for contracting stations to use automated procedures in the evaluation of tenders. The provision must be read in light of the subsequent Art. 30, where it provides for the need, in the case of automated decisions, to ensure both, the knowability and comprehensibility of the decision made, whereby every economic operator has the right to know about the existence of automated decision-making processes concerning him and receive meaningful information about the logic used, and the principle of non-exclusivity of the algorithmic decision, whereby in any case there must remain in the decision-making process a human contribution capable of checking, validating, or refuting the automated decision (on the principles of algorithmic legality, see next paragraph).

Pursuant to the new Code, Art. 23, Legislative Decree No. 36/2023, the National Public Contracts Database is divided into five sections, corresponding to the services offered to contracting stations and economic operators, which may be implemented due to technological development and the availability of data acquired by ANAC. In particular: (i) the Single Registry of Contracting Stations, through which the list and qualification of contracting stations, aggregating entities and central purchasing bodies is managed; (ii) the Computerised Record, through which the sanctions adopted by the Authority relevant to the participation of economic operators in award procedures are published; (iii) the Registry of Economic Operators makes use of the business registry and censuses all economic operators in any capacity involved in public contracts, as well as individuals, natural persons and office holders referable to them; (iv) the registry assumes certification value of the roles and offices held by natural persons not resulting from the business registry; (v) the National Procurement Platform, which interacts with the digital e-procurement platforms used by contracting stations. The Economic Operator's Virtual File that contains for each subject the data and information for the verification of general and special requirements needed to participate in the tender.

The new code envisions a radical change in the system through the creation of a national digital ecosystem within which all administrative processes and fulfillments related to the entire life cycle of public contracts are to be managed.

The real challenge of the new Code is the realization and implementation of the national e-procurement ecosystem, which represents a step forward with no going back, imposing an effective reengineering of the procedures, fulfillments and organization of all operators in the sector, public and private.

With this in mind, there is still a long way to go, and achieving the goal will require loyal cooperation between the authorities responsible for adopting the implementing regulations and the administrations that must ensure the use and interoperability of data, the interconnection of databases, the implementation of infrastructure, the purchase of information tools and the retraining of personnel.

5. The effects of digitization on the activity of public administration: participation, automation and principles of algorithmic rule of law

Procedural participation is provided for by Chapter III of Law No. 241 of August 7, 1990, and encompasses a series of institutions that enable the public administration to make its choices taking into account the reasons of others and the contribution, including collaborative, of interested parties to administrative action[59].

In particular, the participatory nature of administrative action is exercised through the public administration's obligation to communicate the initiation of proceedings (see Articles 7 and 8), through the affirmation of the right of interested parties to intervene in the proceedings (see Article 9), to view the records of the proceedings as well as to submit pleadings and documents (Article 10), to know the reasons that prevent the granting of their requests (Article 10-bis) and the possibility of entering into procedural or substitute agreements (Article 11).

In essence, the activation of an adversarial process between private parties and the administration is a corollary of the principle of due process under which administrative action is aimed at the adoption of measures that

[59] PROIETTI, *La partecipazione al procedimento amministrativo,* in *Codice dell'azione amministrativa*, edited by M.A. SANDULLI, Milan, 2017, 566.

take into account the subjective situations of the target citizens, downstream of their involvement for the presentation of their reasons. This is both to protect the interests of the latter and to better pursue the public interest[60] .

The principle of participation is a direct corollary of the principles of impartiality and good performance enshrined in Article 97 of the Constitution, being participation not only a means of protecting individual interests but also an indirect way of identifying public ends[61] .

The principle is also fully recognized in the supranational legal system as a corollary of the right to good administration enshrined in Article 41 of the Charter of Fundamental Rights of the European Union and has been consolidated as a general canon of administrative activity also thanks to the case law of the Court of Justice.

It should be pointed out that, as regulated by the law of procedure, participation takes on different purposes, both collaborative and defensive[62] : that is, through it the broadening of the facts and interests on which the administration is called upon to pronounce is permitted, as well as the presentation of defensive arguments by the future recipient of the effects of the measure, especially when potentially intended to adversely affect its legal sphere. In the opinion of authoritative doctrine[63] participation is also a source of legitimization of administrative power, since it contributes to the introduction of the interests that the administration will then be called upon to evaluate comparatively.

---

[60] R. CARANTA-FERRARIS, *La partecipazione al procedimento amministrativo,* Milan, 2010, 37.

[61] R. PROIETTI, *La partecipazione al procedimento amministrativo,* cit., 568.

[62] P. CHIRULLI, *La partecipazione al procedimento*, in *Principi e regole dell'azione* amministrativa, edited by M.A. SANDULLI, Milan, 2023; S. BONETTI, *La partecipazione strumentale*, Bologna, 2022, 21.

[63] M.R, SPASIANO, *Nuovi approdi della partecipazione procedimentale nel prisma del novellato preavviso di rigetto*, in *Diritto dell'economia*, 2022, 30.

The participation of the interested parties in the proceedings also pursues deflattive purposes of litigation, as the administered persons can protect their interests directly in the course of the administrative activity, avoiding, in cases where participation develops in a virtuous manner, to wait for the conclusion of the proceedings to interrelate with the administration and, if necessary, challenge the measure before the administrative judge. By intervening at the procedural stage, it is therefore possible to anticipate the reasons for disagreement and the elements that could influence the administration's final determination.

Participation is also along the lines of democratization of administrative action, in that the right of interested parties to participate in the proceedings marks the establishment of an administrative *agere* based on the acquisition of the elements provided by the public and private parties involved in the conduct of administrative action[64] , with the consequence that, where participation is fully carried out, the final measure constitutes a synthesis of all the interests at stake.

Consequently, the issue of participation must be examined both from a guarantor perspective - where the defense of the interests of the subjects involved in the administrative procedure is allowed - and from a functional perspective for the conduct of administrative action, since through participation not only the correct formation of the final decision is realized but also indirectly a form of cooperation of all subjects - public and private - involved in the procedure.

These coordinates, which are inescapable in a rule of law, appear to be strongly questioned-or at any rate must be reconsidered-in the hypotheses of

[64] R. PROIETTI, *La partecipazione al procedimento amministrativo,* cit., 569.

administrative decisions made through the use of algorithms or artificial intelligence systems.

Administrative procedure[65] , indeed, constitutes the core of the positive system that regulates the action of public administrations as a phenomenon of legal significance[66] and guarantees the traceability of public power within a canon of procedural rationality that allows the participation of interested parties in the process of forming the public decision, including for the purpose of controlling the formation of the same[67] . The use of new technologies in the public sector thus poses the problem of balancing the efficiency of administration 4.0 with respect for the guarantees of procedural legality established by Law No. 241/90 and the principle of good administration enshrined in Article 41 of the Charter of Fundamental Rights of the European Union[68] .

Well, as the phenomenon of automation of administrative activity may develop according to distinct degrees of intensity, without being able to enter here into the classification of the various technological solutions that can be used by the public administration, it is sufficient to consider that depending on the role assigned to them, different conclusions will be reached in terms of procedural guarantees from the safeguard. Generally speaking, three levels of

---

[65] Defined in A.M. SANDULLI, *Manuale di diritto amministrativo*, Naples, 1969, 373, as the "*sequence of acts and operations that are carried out with a view to a certain result of administrative law.*"

[66] F. BENVENUTI, *Funzione amministrativa, procedimento, processo,* in *Riv. Trim. dir. Pubbl*., 1952, I, 118.

[67] F. NASSUATO, *Legalità algoritmica nell'azione amministrativa e regime dei vzi procedimentali*, in *Ceridap*, 1, 2022, 151.

[68] D.U. GALETTA, *Digitalizzazione e diritto ad una buona amministrazione*, cit. 85. In general on the principle of good administration in the European context, see R. BIFULCO, *Art. 41. Right to good administration*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (eds.), *L'Europa dei diritti. Commentario alla Carta dei Diritti Fondamentali dell'Unione Europea ,* Bologna, 2001, pp. 290; A. ZITO, *Il "diritto ad una buona amministrazione" nella Carta dei Diritti Fondamentali dell'Unione Europea e nel diritto interno*, in *Riv. it. dir. pubbl. com*, 2, 2002, 425 ff.; D.U. GALETTA, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione*, in *Riv. it. dir. pubbl. com.,* 3-4, 2005, 819 ff.; F. TRIMARCHI BANFI, *Il diritto ad una buona amministrazione*, in M.P. CHITI, G. GRECO (eds.), *Trattato di diritto amministrativo europeo. Parte generale,* Tomo I, Milan, 2007, 49 ff.

automation can be identified[69] : (i) "full" automation can be achieved when artificial intelligence systems are adopted for the adoption of the final measure, without the need for the intermediation of the "natural person" official for the extrusion of the will of the Administration; (ii) alternatively, a level of automation requiring reduced human intervention can be hypothesized, where the official uses the automation system to carry out part of the preliminary activities necessary for the adoption of the final measure and interacts with the system to review or control the result produced by the machine; (iii) finally, a level of automation flanked by a predictive component can be envisaged. These are assumptions based on self-learning predictive artificial intelligence systems (so-called Machine Learning).

It should be pointed out that doctrine and jurisprudence seem to agree that the use of automated tools within the administrative procedure does not constitute an autonomous power, but rather a mere "organizational nodule" of a procedural and investigative nature, thus placed in an exquisitely ancillary and functional position with respect to the concrete extrusion of power[70] .

Well, if the different type of automation (and therefore of technological solution) contemplated seems to have, from the legal point of view, radically different fall-off points with reference to some issues such as that of the imputability of the decision adopted (think of the difference between the hypothesis under (i) where the measure is fully adopted by the machine and the hypothesis under (ii), where instead there remains a margin of contribution

---

[69] D.U. GALETTA-CORVALAN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?*, cit., 9.

[70] On this point, in case law, see Cons. St., Sec. VI, Dec. 13, 2019, no. 8472, § no. 10; in doctrine, ex plurimis, L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Federalismi,* 2, 2018, 10; A.G. OROFINO, *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in Foro amm. C.d.S., 9, 2002, pp. 2256 ff.; F. SAITTA, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, in *Riv. dir. amm. elettr*., 2003, pp. 24 ff.; S. CIVITARESE MATTEUCCI, "*Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità,* in *Dir. Pubbl*, 2019, p. 16.

by the official) a clear differentiation does not appear instead decisive with reference to the exercise of participatory guarantees. This is because, whether we are dealing with fully automated procedures or partially automated procedures (where the IA plays an exquisitely instrumental role in the adoption of the final decision), the problem of reconciling the contraction of the respective procedural phases with the exercise by the interested parties of their participatory prerogatives arises in each case, the latter of which cannot be irremediably (and without legal basis) compressed for the benefit of procedural speed.

The issue of the compatibility of automated administrative decisions with the existing legal framework, in light of a still very meager regulatory framework, has been addressed by administrative jurisprudence[71] which, showing a discreet *favor for the* digitization process for public administration, has dictated some basic tenets on "algorithmic legality"[72] . Specifically, the

[71] See in particular Cons. St., Sec. VI, Dec. 13, 2019, no. 8472; id., Feb. 4, 2020, no. 881.

[72] Contributions on the subject are innumerable. See, without claiming to be exhaustive, E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm*., 2, 2020, p. 281; L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in Federalismi.it, 21, 2018; Id., *Attività amministrativa e intelligenza artificiale,* in *Cib. dir.,* 1-2, 2019, pp. 64 ff.; G. AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Naples, 2019; E. CARLONI, *Algoritmi sulla carta. Politiche di digitalizzazioen e trasformazione dgitale delle amministrazioni*, in *Dir. pubbl.,* 2, 2019, pp. 363 ff; S. CIVITARESE MATTEUCCI, *Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, cit., pp. 5 ff.; F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Dir. pubbl*., 1, 2019, pp. 43 ff.; D.U. GALETTA, J.G. CORVALÁN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?*, cit.,; A. MASUCCI, *Vantaggi e rischi dell'automazione algoritmica delle decisioni amministrative*, in AA.VV., *Scritti in onore di Eugenio Picozza,* Vol. II, Naples, 2019, pp. 1105 ff; A. SIMONCINI, *Profili costituzionali dell'amministrazione algoritmica*, in *Riv. trim. dir. pubbl.,* 4, 2019, pp. 1149 ff.; I.M. DELGADO, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?,* in *Ist. fed*., 3, 2019, pp. 643 ff.; R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data*, pp. 305 ff.; A. MASUCCI, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, in *Dir. pubbl.,* 3, 2020, pp. 943 ff.; A.G. OROFINO, G. GALLONE, *Intelligenza artificiale al servizio della funzione amministrativa: profili problematici e spuinti di riflessione*, in *Giur. it*., 7, 2020, pp. 1738 ff.; B. RAGANELLI, *Decisioni pubbliche e algoritmi: modelli di dialogo nell'assunzione di decisioni amministrative*, in Federalismi.it, 22, 2020; A. SOLA, *Inquadramento giuridico degli algoritmi nell'attività amministrativa*, in Federalismi.it, 16, 2020; S. TRANQUILLI, *Il rapporto pubblico-privato nell'adozione e nel controllo della decisione amministrativa "robotica",* in *Dir. soc*., 2, 2020, pp. 281 ff.; P. OTRANTO, *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, in Federalismi.it, 7, 2021; N. PAOLANTONIO, *Il potere discrezionale della pubblica automazione. Incertezze e stilemi*, in *Dir. amm*., 4, 2021, pp. 813 ff;

Council of State has enucleated a series of principles[73] to which the public administration should conform when using technological solutions, only in the presence of which automated decisions should be considered permissible. Notably, the appellate administrative judge specified the necessary compliance by the public authorities with: i) the principle of knowability of the algorithm; ii) the principle of non-exclusivity of the algorithmic decision; and iii) the principle of algorithmic non-discrimination. These principles would be derived from Regulation 2016/679/EU on the protection of personal data (GDPR), which, in the presence of automated decision-making, recognizes the data subject's right to information and access to that process, the right not to be subjected to a decision based solely on automated processing, as well as the guarantee regarding the non-discriminatory nature of the procedures.

The aforementioned principles, the result of an essentially creationist thrust of administrative jurisprudence[74] , aim *de facto at* strengthening the procedural guarantees enucleated in l.n. 241/90, in order to offer greater protection to the recipients of automated administrative action, believing that the "traditional" rules are not sufficient to achieve this purpose and may generate gaps in protection. The principles of algorithmic legality would thus aim to supplement the procedural guarantees provided by the general law on administrative procedure, with a view to transparency and comprehensibility of the tool used as well as the need for human intervention in the procedure carried out. These would be, in essence, true rules of procedural legality suitable for establishing in the recipients of administrative action "a new generation of procedural claims" that would complement those provided for in

[73] According to POLICE, *Scelta discrezionale e decisione algoritmica, cit.*, 498, rather than actual principles, they would be "*more modestly corollaries of the application of the principle of legality of the actions of public authorities.*"

[74] See infra § 4.

Law No. 241[75]. To this it should be added that, as concurringly stated in doctrine[76] , these would be “strengthened” procedural guarantees for which, in case of omission by the administration, the applicability of dequotation to “non-invalidating defects” would be excluded by virtue of the second paragraph of Article 21-octies of Law No. 241/90.

At this point, prescinding from the specific examination of the corollaries of “algorithmic legality” coined by administrative jurisprudence, we intend to dwell only on the profiles exquisitely pertaining to procedural participation in order to identify possible limitations and critical issues.

On algorithmic transparency, it has been argued that the citizen's understanding of the rule guiding the decision must be ensured, even when it is expressed in a language other than legal language, and its traceability must be ensured. Knowledge of the algorithm must therefore be ensured in all its aspects: from its authors to the process used in its elaboration, to the decision-making mechanism, including the priorities assigned in the evaluation and decision-making procedure of the data selected as relevant[77] . Now, leaving aside the analysis of the critical issues concerning the intellectual property rights claimed by those who provided the administration with the software adopted for the decision[78] , it cannot but be noted that mere access to the "source code" does not always put the interested party in a position to understand the logical process underlying the administration's decisions[79] .

---

[75] E.N. FRAGALE, Cittadinanza *amministrativa al tempo della digitalizzazione*, in *Dir. amm*., 2, 2022, 501.

[76] F. NASSUATO, *Legalità algoritmica*, cit. p. 164.

[77] See Cons. St., sec. VI, no. 2270, 2019.

[78] On this topic see, ex plurimis, F. BRAVO, *Trasparenza del codice sorgente e decisioni automatizzate*, in Dir. Inf. and Inf., 2020, I, 694.

[79] Interesting is the distinction made in COGLIANESE-LEHR, *Trnasparency and Algorithmic Governance*, in *Administrative Law Review*, 2019, I, 1, between "fishbowl transparency" and "reasoned transparency" where the former case is aimed merely at "showing" the administration's work and the latter pertains more deeply to the profile of the comprehensibility of public action.

Furthermore so if we understand transparency as referring not exclusively to the final measure, but to the entire procedure, here it is an effective instrument of participation for the administered[80] .

Precisely, with reference to this last profile, the solution adopted in the French legal system appears convincing, where in the Loi pour une Republique numerique of 2016 it is provided that the administration has, among other things, the obligation - at the request of the interested party - to communicate the operating rules and characteristics of the algorithm and in particular the degree and manner of contribution of the algorithmic processing to the decision-making process, the parameters and conditions of the algorithmic processing of information and the possible mechanism for weighting data and information, as well as the set of operations carried out concretely by the algorithm. To this it should be added that administrations are required to publish the list of algorithms used in carrying out their activities[81] .

In concurrent profile, the principle of algorithmic non-exclusivity, which can be derived from Article 22 of the GDPR, relates to the necessary human intermediation in the adoption of automated decisions according to the model of the so-called *human in the loop*, according to which in order to produce its result it is necessary for the machine to interact with the human being[82] . In this sense, then, in the administrative procedure, automation configures a dynamic of the human-machine role that is one of subsidiarity and complementarity, which implies a renewed role of the figure of the person in charge of the procedure who, in the conduct of the automated process, becomes

---

[80] A. CORRADO, *Conoscere per partecipare: la strada tracciata della trasparenza amministrativa,* Naples, 2018, *passim.*

[81] L. TORCHIA, *Lo Stato Digitale. Una introduzione*, cit. 120.

[82] On the topic see S. CIVITARESE MATTEUCCI, "*Umano troppo umano",* cit., passim; as well as, most recently, GALLONE, *Riserva di umanità e funzioni amministrative,* Padua, 2023.

the primary guarantor of this embankment to a depersonalized management of the procedure[83] . Well, it is desirable that in this context the person in charge of the procedure assumes a crucial role for participatory purposes, since he or she is the referent of the interested parties and provides information on the progress of the procedure as well as any indication about the functioning of the algorithm, being also able to translate its content into intelligible language so as to explicate its dynamics[84] .

In this scenario, the role of the person in charge of the procedure as guarantor of procedural participation and interlocution between the administration and citizens would bring out the close interconnection between the rules on the person in charge of the procedure and those governing the intervention of the interested parties and the adversarial process with the proceeding administration (Articles 7 et seq. of Law No. 241/90)[85] . And it is precisely for the purposes of participation that the mediation of a "natural person" official in the proceedings appears to be as essential as ever, at least at the stage of ascertaining the factual and legal prerequisites necessary for the adoption of the automated measure[86] .

It is therefore possible to assume that procedural participation constitutes a guarantee of fair automated procedure, and its centrality is all the more strengthened if one considers that the implementation of participatory guarantees could at the same time democratically legitimize automated administrative decisions, since they are based on the consent of the

---

[83] D. MARONGIU, *Aloritmi e procedure amministrative: una ricostruzione*, in Giur. It., 2022, 1520.
[84] D. MARONGIU, *Algoritmi*, cit. 1521.
[85] F. NASSUATO, *Legalità algoritmica*, cit. p. 171.
[86] N. PAOLANTONIO, *Il potere discrezionale della pubblica automazione.,* cit., 831, where it is significantly stated that "*the more indeterminate the norm to be applied or the more complex the reality on which the algorithm has to operate, the more human intervention is necessary: taking care of the preliminary investigation, adopting any procedural relief, even preparing the outline of the measure.*"

administered that is expressed through the collaborative input and interlocution with a human official (at least at one of the stages of the procedural process)[87] . To this it should be added that the confrontation between the public administration and private parties during the course of the procedure will enable the former to become fully acquainted with the peculiarities of the concrete case that will be represented to it by the private parties and to take them into account downstream of the automated decision also as a parameter of the latter's referability to the concrete case.

For these reasons, the relationship between procedural participation, the necessary intervention of the human manager and the prohibition of fully automated procedures would hinge an instrument of substantive guarantee for the recipients of administrative action, which, however, would conflict with the hypothesis of implementing adversarial debate only at the final stage of the procedure, that is, making it focus on a decision outline already prepackaged by the algorithmic tool. This, as has been observed, would distort the main function of the participatory institute, namely that of "*establishing a regime of communication from which a 'draft' decision can emerge*" based on the prior acquisition and selection of the interests involved, starting with the obligation, incumbent on the administration, to evaluate the pleadings and documents produced by the interveners, if they are relevant to the subject matter of the proceedings.

Having identified the principles (*rectius*, corollaries of the principle of Rule of Law)[88] that should permeate the procedures connoted by a certain rate of automation, it is necessary to ask how these are reconciled, in practice, with

---

[87] I. ALBERTI, *Parteciapzione procedimentale per legittimare gli algoritmi nel procedimento amministrativo*, in R. CAVALLO PERIN (ed.), *Pubblica amministrazione con I big data*, *cit.*, pp. 285 ff; NASSUATO, *Legalità algoritmica*, cit., p. 173.

[88] See footnote 24.

the traditional institutes of participation such as the notice of initiation of proceedings, procedural pleadings or the notice of rejection enucleated by Law No. 241/90. An operation of fundamental importance[89] that must, however, be carried out by the interpreter, we are reminded, in the absence of unambiguous normative indications.

On this point, it is argued that in a digitized context the notice of initiation of proceedings should find fewer and fewer exceptions[90] and, at the same time, may have new contents intimately related to the fully or partially automated nature of the proceedings initiated. In this regard, it has been thought, in the wake of the French system and in application of the chrisms deriving from the GDPR, that it may be appropriate to include in the communication in addition to what is indicated in Article 7 of l.n. 241/90 (appropriately supplemented by Article 12, paragraph 1, lett. d) of d.l. no. 76/2020, by which it was added ne need to indicate in the notice of initiation of the procedure also the digital domicile of the proceeding administration) also all the elements suitable to comply with the aforementioned principle of knowability of the algorithm, always in the desired logic of a "reasoned" transparency[91] . We refer specifically, in addition to the crude indication about the fact that the procedure will be managed (in whole or in part) by an algorithm or an AI system, to the degree of automation of the procedure itself, to the mode of operation of the system used, to the inputs entered into the machine, to the weights and measures indicated to it, to the inferences expected

[89] R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data*, cit. 317, where it is argued that "*the regulation of the informative administrative act does not make any derogation from the indicated principle* [of legality]*, but on the contrary poses an explicit reinforcement of the now coessential principle of participation of the interested parties in the administrative procedure leading to the issuance of a measure.*"

[90] D.U. GALETTA, *Digitalizzazione e diritto ad una buona amministrazione*, cit., 95.

[91] See footnote 30.

and to any other element suitable for making the citizen understand the logic underlying the initiating procedure.

Once the procedure has been initiated, the problem arises as to how to develop (and at what moment to place it) the procedural adversarial process, the automated procedure being evidently characterized by a compression and an overcoming of the division into "phases" that characterizes traditional procedures (of the initiative, inquiry and decision-making). In this regard, the possibility of opening the adversarial process at the moment between the adoption of the automated decision and its transformation by the physical person official into the final measure (this assuming that the final measure cannot be adopted directly by the machine consistent with the necessary human intermediation according to the human in the loop model) appears undoubtedly agreeable, as well as compatible with the principles of knowability and non-exclusivity mentioned before. On this point, it has been significantly argued that the algorithmic decision can thus be legitimized by the "*notice and comment*" (typical of regulatory measures taken by *authorities*), generalizing the prior consultation of stakeholders on the "proposed measure" given by the algorithm[92] . Well, the notice on the outcomes arrived at by the algorithm would constitute the moment in which to open the adversarial stage with the interested parties, with the required human interposition invoked by doctrine and jurisprudence and the possibility of: i) confirming the determinations of the machine, ii) providing for an exception or iii) ordering its correction. The described adversarial phase on the proposed measure would not configure *ex ante* an aggravation of the procedure ex art. 2, l.n. 241/90, favoring on the contrary the integration of the algorithm, or its correction, constituting that

[92] R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data,* cit., 320.

investigative or evaluative activity indispensable for the exercise of the participatory prerogatives of the interested parties.

It follows from this that the algorithmic procedure and the resulting automated act find a "legal basis" and general legitimacy by interpreting in conjunction of the institutions provided by the general law on administrative procedure (see in particular Articles 7, 8, and 10-bis), with the general discipline of effectiveness of the right of data subjects to obtain human intervention in Article 22 of the GDPR[93] .

In conclusion, the use of decision automation tools, from which derives a necessary temporal concentration of the constituent phases of the administrative procedure, cannot result in a compression of the participatory guarantees recognized by law to protect the subjective legal situations related to the exercise of power[94] . Preliminary interlocution with the person in charge of the procedure, exchange of pleadings and documents, participatory access, comments on the rejection notice, must necessarily be guaranteed, albeit in the partially different forms described in the previous paragraph. It is extremely important that these rules retain their centrality because in a rule of law procedural guarantees are in themselves very important, at least as important as the substantive interests that administrative activity is intended to satisfy[95] . This necessitates the need for an “updating” of the traditional institutions of participation aimed at their adaptation to the peculiarities of procedures managed through the use of new technologies. A significant step forward in this direction has been taken in our country by administrative jurisprudence,

---

[93] R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data,* cit., 321.

[94] V. NERI, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in Urb. and App., 2021, 5, 581.

[95] D.U. GALETTA, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione,* in *Riv. It. Dir. Pubbl. Com.*, 2005, 3, 819.

which with a *necessarily* creative approach has coined the corollaries of algorithmic legality mentioned above, which will undoubtedly inspire the work of interpreters in the times to come.

CHAPTER II

CYBERSECURITY IN THE PRISM OF PUBLIC PROCUREMENT LAW: AN ATTEMPT TO RECONSTRUCT THE RULES OF THE GAME BETWEEN PARTICIPATION REQUIREMENTS, AWARD CRITERIA AND CERTAINTY REQUIREMENTS.

SUMMARY: 1. Background. Public Administration, digital transition and PNRR: the role of private entities. 2. Cybersecurity among new challenges for the State: what implications for public procurement law? Delimitation of the field of inquiry. - 3. Cybersecurity in the source of law system. 4. Cybersecurity as award criteria: lights and shadows of the changes brought by the new Public Procurement Code. 5. Compliance with cybersecurity *standards* as a substantial market access criterion. - 6. First concluding remarks.

1. Background. Public Administration, digital transition and PNRR: the role of private entities

In recent years, a number of issues have emerged that public actors need to address, such as the idea of cyberspace as a public good[96] global, the danger of algorithm-dominated decision-making processes, as well as the damage so-called fake news and disinformation can cause to both individuals and society as a whole. Technological advancement, dubbed by some as a revolution[97] has, on the other hand, always prompted new representations of the "machina machinarum" state[98] . To this day, the very sovereignty of states is being

[96] On the concept of public good see, among all, A.M. SANDULLI, *Beni pubblici,* in *Enc. dir.*,V, Milan, Giuffre`, 1959; S. CASSESE, *I beni pubblici. Circolazione e tutela*, Milan, Giuffre`, 1969.

[97] L. Floridi, *La rivoluzione dell'informazione*, Turin, Codice Edizioni, 2012.

[98] L. Casini, *Lo Stato nell'era di Google,* Milan, Mondadori, 2020, 48 and the contributions cited therein on the subject including N. Irti, *Lo Stato: machina machinarum*, in *Riv. Trim. Dir. Pubbl*., 2004, 309.

challenged by what has been called, with an oxymoron, the "private sovereignty" of planetary-scale enterprises[99] . In this context, public law must prepare effective countermeasures, as it is increasingly forced to chase a very rapidly changing reality that would instead require timely reactions from national and supranational institutions.

New technologies, from the web, to 5G connections, artificial intelligence, blockchain, and the metaverse, create new market contexts, generate lifestyles, and initiate new ways of relating people and things. These are radical changes that mark an epoch in the evolution of humankind[100] .

In this context, the public administration plays multiple "parts in the play." It, just like the community, undergoes technological evolution and is affected by it; however, it often uses it to carry out its functions; finally, it attempts to exercise the essential regulatory activity against it. [101]

With reference to this evolutionary process, some authors have begun to speak of a “Digital State”[102] which, while continuing to perform its traditional

---

[99] M. Clarich, *Prefaziome*, in A. Lalli, *La pubblica Amministrazione dell’era digitale*, Turin, Giappichelli, 2022, XIV.

[100] Y.N. Harari, *Homo Deus, breve storia del futuro*, Milan, Bompiani, 2018.

[101] A. Lalli, *Introduzione*, in A. Lalli, *Pubblica Amministrazione nell’era digitale,* cit., XVI. On the subject of the use of new technologies in the service of the public sphere, see also *Report on the Main Problems of State Administration* presented to Parliament on November 16, 1979 by then Minister of Public Service M.S. Giannini. Reference taken up in A. POLICE, *Scelta discrezionele e devcizioni alrogirmiche*, in *Il diritto nell'era digitale*, edited by GIORDANO, PANZAROLA, POLICE, PREZIOSI AND PROTO, Milan, Giuffré, 2022, 496. For an in-depth examination of the Report, see D'AURIA, *Giannini e la riforma amministrativa*, in *Riv. Trim. dir. Pubbl.,* 4, 2000, 1209.

[102] L. Torchia, *Lo Stato digitale*, cit.. In the same vein, on the concept of "Public Administration 4.0" see D.U. GALETTA AND J.G. CORVALAN, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? cit.*, where the authors, reconstructing the path of technological development of the p.a. effectively State that "*in the 20th century, the evolution of information and communication technologies (ICT) has shaped an asymmetric combination between three paradigms of Public Administration: Public Administration 1.0, which corresponds to the classic Public Administration model of the 19th century, characterized by the use of paper, printing and typewriter. Public Administration 2.0, which incorporates computers, text processors, printer and fax machine. Public Administration 3.0 to which, in the 21st century, the public sector has begun to migrate through the use of the Internet, digital portals, mobile applications and social networks. Currently, however, Public Administration is already in a fourth phase of evolution. This fourth phase is related to the so-called Fourth Industrial Revolution and has as its lowest common denominator a high degree of automation*

functions presents at least two new features compared to the past. In one respect, public activity as a whole is being transformed, both in ways and means, through the application of new technologies[103] . In essence, whether it is security or public services, infrastructure construction, currency, defense, health, or territorial government, the use of technological tools is required, and this phenomenon calls for the redefinition of the rules of exercise of public power and the related modes of control.

In competitor profile, technological development invests economic and social relations to such an extent that existing rules are often unsuitable and obsolete. Hence the need for new public regulation aimed at updating existing disciplines, and introducing principles and rules that adapt to such new phenomena, as is happening with digital services and the application of artificial intelligence[104] .

Given the inescapable need for a digital transition of public administration, it has been placed at the center of investments related to the Next Generation Eu[105] . With reference to the Italian context, specifically, the National Recovery and Resilience Plan[106] dedicates a specific Mission (called M1C1 - "Digitalization Innovation and Security of PA," included in the general

---

and interconnectedness that is exerting a major impact on human beings themselves and their way of being, as well as on their environment of reference."

[103] On the phenomenon of digitization of public administration see, *ex plurimis,* without claiming to be exhaustive, *Il diritto dell'Amministrazione Pubblica digitale*, edited by D.U. GALETTA and R. CAVALLO PERIN, Turin, Giappichelli, 2020; R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm*, 2, 2020, 305 ff; Id., *Pubblica Amministrazione con i big* data, cit. *passim*; L. TORCHIA, *Lo Stato digitale,* cit., *passim*; A. Lalli, *La Pubblica Amministrazione nell'era digitale*, Turin, Giappichelli, 2022.

[104] L. TORCHIA, *Lo Stato digitale,* cit., 19; from the normative point of view, we refer to the Draft Regulation being approved by the European Parliament and the Council, aimed at establishing harmonized rules of artificial intelligence. The text of the proposal formulated by the Commission (COM(2021) 206 final) is available at the following link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52021PC0206.

[105] https://next-generation-eu.europa.eu/index_it

[106] Available at the following link: https://www.governo.it/sites/governo.it/files/PNRR.pdf. For a legal framing of the instrument see, *ex plurimis,* M. Clarich, *The PNRR between European and national law: an attempt at legal framing*, July 2021, in Corriere Giuridico, no. 8-9/2021, 1025 ff.

Mission "Digitalization, Innovation, Competitiveness, Culture and Tourism") to which about twelve billion Euros of investments are dedicated. In this area, a national *cloud* infrastructure is being developed, on which the data stored by the member public administrations (National Strategic Pole) will migrate[107] , but also a National Digital Data Platform that will make possible the interoperability of the information systems of public administrations and public service providers through the accreditation of the qualified entities[108] .

To live up to the needs of the community, the administration's digital transition process must inevitably materialize in its use of artificial intelligence systems, *software*, *data computing* and *blockchain* platforms. In most cases, administrations do not have in-house expertise to integrate these tools into their infrastructure, which inevitably leads them to turn to the *outsourced* market[109] .

This trend places the dialectic between the public and private sectors, between government and large companies specializing in the implementation of high-tech solutions, at the center of the debate. Indeed, the latter are called upon to contribute to the pursuit of the public interest through the provision of suitable tools to guide the public sector's digital transition. According to some authors, there is a real relationship of subordination of the public sector to the private sector[110] that is rooted in the inability of public administrations to

---

[107] G. NAPOLITANO, *Il partenariato pubblico-privato per l'implementazione del Polo Strategico Nazionale*, in Giorn. Dir. Amm., 6/2021, 703-707.

[108] A. SANDULLI, *Pubblico e privato nelle infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513. For a timely numerical examination of the increase in public ICT investment, see Report 1/2023 "*ICT Spending in the Italian PA 2022. Main trends and ongoing paths"* available at the following link: https://www.agid.gov.it/sites/default/files/repository_files/26_07_rapporto_spesa_ict_2022.pdf

[109] D.U. GALETTA, *Transizione digitale e diritto ad una buona amministrazione*, cit., 109 as well as the contribution cited therein MARY C. LACITY-RUDY HIRSCHHEIM, *Information systems outsourcing; Myths, Metaphors and Reliabilities*, John Wiley & Sons Ltd, England, 1993.

[110] A. NATALINI, *Come il passato influenza la digitalizzazione delle pubbliche ammijnistrazioni*, in *Riv. trim. dir. pubbl.,* no. 1, 2022, 95; A. SANDULLI, *Pubblico e privato nelle infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl*., 2021, 513.

formulate their digital transformation strategies and identify the technological tools needed to implement them. Added to this is the fact that the *Information and Communication Technologies* (so-called ICT) market has been characterized by very strong concentration and is now dominated by a few multinational players[111] . These circumstances, in essence, place government and international *big tech* in a state of mutual interdependence. Indeed, on the one hand, big companies base an increasingly large part of their *business* on institutional orders; on the other hand, we repeat, the digital transition process of public administrations would be difficult, if not impossible, without the contribution of private technology partners[112] .

In this context, where we move in the direction of a *Governement as a Platform* model[113] in the face of the significant benefits that may be generated in terms of growth, there will also arise for governments (and for administrative law scholars) the need to think about a resilient regulatory framework, capable of adapting to the speed of change produced by the digital transition[114].

2. Cybersecurity among new challenges for the State: what implications for public procurement law? Delimitation of the field of inquiry

[111] On this topic, see L. CASINI, *Lo Stato nell'era di Google*, in *Riv. Trim. Dir. Pubbl.*, 2019, 1125, where the author highlights The different aspects of the influence of big companies (especially the tech sector) on democratic systems. On the topic see also, M.R. FERRARESE, *Poteri nuovi,* Bologna, Il Mulino, 2023.

[112] For a reconstruction of the new ordinamental arrangements in this area see O. POLLICINO, *Potere Digitale*, in *Enciclopedia del Diritto*, *Tenatiche*, V - 2023, 410 ff., where the author speaks of the "transfiguration" of private subjects from economic actors to powers in the strict sense.

[113] B. BOSCHETTI, *La transizione digitale della pubblica amministrazione verso il modello Governement as a platform*, in A. LALLI, *Pubblica Amministrazione nell'era digitale*, cit. 5.

[114] B. BOSCHETTI, *La transizione digitale della pubblica amministrazione verso il modello Governement as a platform*, cit. p. 42.

In light of the above, it should be noted that digital infrastructures constitute an essential instrument through which the public interest is pursued and subjective legal situations are protected, in relation to their use in the exercise of administrative functions and the provision of public services[115] . Consequently, it is necessary to protect the aforementioned infrastructures from cyber attacks or incidents, precisely because of their instrumentality with respect to the protection of the public interest as well as the positions of the administered[116] .

Cybersecurity is defined as "*the set of activities necessary to protect the network and information systems, users of those systems, and others affected by* cyber *threats*"[117] .

The topic presents considerable complexities. It is an area intimately connected with the galloping technological progress that characterizes our times, a circumstance that has meant that the law and protection procedures have often trudged before the speed with which *vendors* offer customers (*i.e.,* Administrations and all citizens in general) simple and immediately usable

---

[115] S. ROSSA, *Cybersecurity e pubblica amministrazione,* Naples, Editoriale Scientifica, 2023, 27.

[116] As highlighted in B. CAROTTI, *Sicurezza cibernetica e Stato,* in *Giorn. Dir. Amm*., 5, p. 629, the design of a State strategy that takes into account both the "protection" of domestic infrastructures and their placement within the European context is an issue intimately connected to that of the exercise of *golden power*, on which, unable to dwell here, see, among others, A. SANDULLI, *La febbre del golden power*, in *Riv. Trim. Dir. Public,* 3, 2022, 743; G. DELLA CANANEA, L. FIORENTINO (eds.), *I "poteri speciali" del governo nei settori strategici*, Naples, Editoriale Scientifica, 2020; G. NAPOLITANO (ed.), *Foreign Direct Investment Screening, il controllo sugli investimenti esteri diretti,* Bologna, il Mulino, 2019. G. NAPOLITANO, *L'irresistibile ascesa del golden power e la rinascita dello Stato doganiere*, in *Giorn. Dir. Amm.,* no. 5, 2019, p. 551; M. CLARICH, *La disciplina del golden power in Italia e l'estensione dei poteri speciali alle reti 5g*, in G. NAPOLITANO (ed.), *Foreign Direct Investment Screening*, op. cit, p. 118.

[117] Art. 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council of April 17, 2019 on ENISA, the European Union Agency for Cyber Security, and on cybersecurity certification for information and communication technologies, and repealing Regulation (EU) No. 526/2013 ("Cybersecurity Regulation"). Definition later taken up by Art. 1 of dl 82/2019, under which cybersecurity is defined as "*the set of activities, (...), necessary to protect networks, information systems, computer services and electronic communications from cyber threats, ensuring their availability, confidentiality and integrity and ensuring their resilience, including for the purpose of protecting national security and national interest in* cyberspace."

technological solutions[118] . The issue has been brought to the forefront of the debate by the European legislature, which has made it clear that "*Digitization and connectivity are becoming key features of an ever-increasing number of products and services, and with the advent of the Internet of Things (IoT) an extremely large number of connected digital devices are expected to be available throughout the Union in the next decade. Although an increasing number of devices are connected to the Internet, security and resilience are not sufficiently built into the design, making* cybersecurity *inadequate.*"[119] .

In talking about cybersecurity, there are some central concepts that are useful in sketching its boundaries: "pervasiveness," "vulnerability," "security," and "resilience."

As mentioned above, in the process of "digital transition" of public administration progressively and increasingly widespread technology has "pervaded" public digital infrastructure. This places the development and growth of states in an irremediable condition of dependence on technological solutions implemented and provided by private entities. This phenomenon, moreover, will be progressively more and more perceptible, also in light of the substantial resources allocated to the digital transaction of pA by the National Recovery and Resilience Plans already mentioned.

Well, in the face of the profound benefits that the digital transition of public infrastructures brings, it cannot be overlooked that greater pervasiveness of new technologies inevitably corresponds to greater

---

[118] B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato*, in Federalismi, no. 14/2020, 12.

[119] Recital No. 2, Regulation (EU) 2019/881, where it is also clarified that "*In this context, the limited use of certification means that individual users, in organizations and companies have insufficient information about the characteristics of ICT products, ICT services and ICT processes in terms of cybersecurity, which undermines trust in digital solutions. Network and information systems are able to help us in all aspects of life and boost the Union's economic growth. They are critical to achieving the digital single market.*"

vulnerability of the very infrastructures to which the technological solutions are subservient.

Within this general framework, it is therefore clear that not only individuals and companies are at risk but, more broadly, the common good of national security itself can potentially be considered in serious danger leading some scholars to consider national cybersecurity as a "public good"[120] . One thinks of the dramatic consequences that could result from altering the systems that regulate major transportation lines, energy networks, telecommunications networks, or even the health care system, significantly impacting a country's economic sphere, severely affecting its national interests, or even from tampering with modern military defense and government security command and control systems[121] .

This context significantly reverberates on the dialectic between public and private actors: the state invests in the innovation sector to stimulate the development of new technological solutions (see, *ex multis*, PNRR and enterprise 4.0); the state in turn is the first user of the aforementioned solutions (software, databases, artificial intelligence systems, *cloud computing*), which inevitably accompany the public administration in the digital transition process; in turn, both the state and private companies involved in strategic infrastructure actively participate in the implementation of the cyber defense strategy. On this point, the document bearing the "National Cybersecurity

---

[120] R. BRIGHI-P.G.CHIARA, *Cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in Federalismi, no. 21/2021; M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds & Machine*, 2019, 9.

[121] The CLUSIT Association's *2023 Report on ICT Security in Italy* States that "*between 2018 and the first half of 2023, the sample included 1"185 known attacks of particular severity involving government entities around the world. After a particularly significant growth between 2019 and 2021, the number of serious attacks remained almost constant in 2022, only to rise again significantly in the first half of 2023.Over the five-year period, however, it rose from 15.8 attacks per month in 2018 to 21.5 in the first half of 2023, an overall increase of 36 percent.*"

Strategy," published by the Italian Council Presidency in May 2022[122] , states that transversal to the objectives of the strategy is the public-private partnership, marked by "*a whole-of-society approach, which sees the public sector acting synergistically with the private sector, academia and research, the media, families and individuals to strengthen the cyber resilience of the nation and society as a whole. The cyber space, moreover, consists of ICT products and services made or delivered mainly by private entities. For this reason, this strategy cannot do without full collaboration and constant public-private consultation, (...).*"[123].

In such a scenario, significant critical issues arise from the strong information asymmetry that characterizes the public-private relationship, where companies that provide technological solutions to the Administration guard highly specialized *know-how*, not even minimally comparable to the basic preparation of most of the public entities that will have to select, purchase and use those assets. This gives private economic operators, at times, the power to negatively affect the duty/freedom of choice of supplier by the contracting

[122] https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza.

[123] Also in the UK *Governement Cyber Security Strategy 2022-2030*, is pointed out that a a main goal is the development of the «*right cyber security skills, knowledge and culture*». Specifically, in the document is clarified that the Cyber Security Strategy and aim will not be possible without cultivating the required cyber security skills and knowledge, as well as fostering a cultural shift in cyber security across the whole of government. To better manage the new challenges the public sector, indeed, should have a comprehensive understanding of its cyber security skills requirements and incentivise and promote government cyber security careers. As well as formal career pathways, working towards the adoption of a single pay framework for the cyber profession will enable government to more effectively attract, develop and retain those skills, providing a sustainable government cyber security profession. It is crucial for the UK Government, in other words, to stimulate the development of careers and professionalities linked to the cyber world, with the achieve to enrich the cyber resilience of the entire public sector. From the Digital, Data and Technology (DDaT) profession through to government's commercial and legal functions, suff cient cyber security knowledge and awareness will ensure that cyber security is actively considered wherever necessary. In substance, this approach recognises the importance of cultivating a cyber security culture that empowers its people to learn, question and challenge to drive continuous improvement. This begins with improving cyber security awareness and knowledge across all public sector workers, building on these foundations to create a positive cyber security culture that promotes and empowers its people to proactively engage on organisational cyber security risks. Getting this right is the key to sustainable change.

station[124] . More specifically, in relation to the ICT market, one of the typical consequences of information asymmetry between contracting stations and private companies is the so-called *lock-in*[125] , which consists of "*the phenomenon whereby an administration cannot easily change supplier when a contract expires because essential information about the IT system in use, which would allow another supplier to take over from the previous one efficiently, is not available*"[126]. This phenomenon, which typically characterizes the public procurement market in the technology sector, constitutes a pathological effect of the aforementioned information asymmetry, by virtue of which it can happen that the contracting authority, after selecting the company supplying the technological solution, has to incur very high transactional costs if it decides to change supplier, thus finding itself "locked-in" in a condition in which the previously made determinations negatively impact the natural execution of the public contract.

The described critical contractual issues must, moreover, be balanced with the overriding need of public entities to procure secure and cyber-resilient technological solutions. This need implies that the described dialectic between public and private actors is enriched by an additional edge. The main derivative

---

[124] For a careful reconstruction of the phenomenon of information asymmetry in the context of procurement for the provision of ICT services, also with references to studies in political economy on the subject, see S. ROSSA, *Cybersecurity e pubblica amministrazione, cit.*, 51, where the author clarifies that "*information asymmetry occurs when one party has more information (quantitative aspect) or more useful information (qualitative aspect) than another. In this case, the information gap that is created is likely to affect market exchanges in favor of the more or better informed party. There can be two hypotheses of information asymmetries, depending on whether they materialize before or after the conclusion of the agreement.*" We also note the doctrine that has dealt with the issue of information asymmetry in economics including J. Stiglitz, *Information and the Chance in the Paradigm of Economics*, Prize Lecture, December 8, 2001; G.A. AKERLOF, *Market Signaling. Informational transfer in hiring and related screening processes*, Harvard University Press, Cambridge, 1974 .

[125] On this topic see, *ex multis*, G. CARULLO, *Principio di neutralità tecnologica e progettazione* dei *sistemi informatici della pubblica amministrazione,* in *Cib. Dir.*, 1/2020, 33 ff.; A. LICASTRO, *La riscoperta del'abuso di dipendenza economica nell'era dei mercati digitali*, in *Federalismi*, no. 13/2021, 118 ff.

[126] The definition given in the text was formulated by the European Commission in *Against lock-in: building open ICT systems by making better use of standards in public procurement, Com (2013) 455 final, June 25, 2013.*

of sovereignty, i.e., public safety[127] in cyber space requires a strategic approach based not only on regulation but also on the defense of relevant public interests through an interrelationship of national and supra-national, public and private stakeholders[128] .

In the regulation of the process of acquisition of technological solutions by public administrations, a strategic and collaborative approach between public and private actors, between national and supranational institutions is therefore required[129] . The objective of this contribution is to analyze through the lens of public contract law the evolution of the relationships between public actors and private companies contributing to the "technological transition" of the public administration, in order to identify the tools necessary to pursue the difficult balancing act between the different interests at stake (public security and protection of critical infrastructures, on the one hand, and protection of the interests of private companies, the principle of competition and access to the public procurement market, on the other), assessing the adequacy (or not) of the reference legal framework, reasoning on its possible further evolutions. In particular, in the following paragraphs, following a brief reconstruction of the legal context of reference, attention will be focused on the discipline recently

---

[127] On the subject see G. CORSO, *L'ordine pubblico,* Bologna, Il Mulino, 1979; R. URSI, *La sicurezza pubblica*, Bologna, Il Mulino, 2022.

[128] I. FORGIONE, *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni , tra regolazione europea e interna*, *Dir. Amm*, 4, 2022, 1114. On this point, see also R. URSI, *Cybersecurity come funzione pubblica*, in *La sicurezza nel cyberspazio*, edited by R. URSI, Franco Angeli, Milan, 2023, pp. 17, where the author argues that "*if the defense of the cyber "fort" moves, on an objective and subjective level, along the lines of the national security function and military defense, the activity of prevention, aimed at ensuring the resilience of the information system with respect to potential threats, represents a new function for which a public task is identified, in which regulation and administrations take on peculiar connotations, and an organizational architecture, which is distinguished by a composite model in which public subjects with authoritative powers and forms of cooperation with private subjects coexist.*"

[129] L. CASINI, *Lo Stato nell'era di Google,* Milan, Mondadori, 2020, 48, where he cites Y.N. HARARI, *21 lezioni per il XXI secolo*, transl. it., Milan, Bompiani, 2018, 184, according to which to the challenges posed by new technologies to States there can be no exquisitely nationalist response since, as in the case of climate change, "*also for the technological revolution the nation-State is simply the wrong frame in which to frame the threat*."

introduced by the legislature on public contracts (Legislative Decree No. 36 of March 18, 2023), examining the wording of Article 108 of the new Code, which introduces the concept of cybersecurity among the award criteria, as well as the other special provisions that impose *de facto* requirements for participation in tenders aimed at the procurement of technological solutions by public administrations. This is in order to attempt to reconstruct the "rules of the game" with which economic operators must interface in participating in the tenders described, highlighting the major critical issues of the current scenario and reasoning about possible evolutions *de iure condendo.*

3. Cybersecurity in the source of law system

The subject of cybersecurity emblematically reflects the multilevel arrangement that characterizes the legal systems of our time[130] . In the definition of the legal framework[131] , indeed, European legislation has been a driving force in identifying neuralgic profiles and in promoting a unified approach[132] .

Initially, the EU's effort was to establish an agency specifically for cybersecurity issues, without intervening with legislation or requirements binding on member states. Specifically, in 2004 EC Reg. No. 460/2004[133] established the European Network and Information Security Agency (ENISA). The approach of the regulation was very respectful of member states'

---

[130] On the framing of the concept of multilevel order see, *ex plurimis*, M. CARTABIA, *La tutela multilvello dei diritti fondamentali. Il cammino della giurisprudenza della Corte Costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona*, in cortecostituzionale.it, 2014, available at https://www.cortecostituzionale.it/documenti/convegni_seminari/RI_Cartabia_santiago2014.pdf.

[131] Described not surprisingly as "alluvial and multilevel" in R. URSI, *Cybersecurity come funzione pubblica,* cit. p. 18.

[132] For a reconstruction of the relevant legal context see S. Rossa, *Cybersecurity e pubblica amministrazione, cit.*, 65 ff.; E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica*, Turin, Giappichelli, 2023, 87 ff.

[133] Reg. (EC) March 10, 2004, No. 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency.

prerogatives[134] and essentially ENISA was set up as a technical body to assist the European Commission and each state. It was not until 2019, with Regulation EU/2019/881 (the so-called *Cybersecurity Act*), that ENISA took on a more operational role, on which we will elaborate *below*.

An initial regulatory framing of the architecture of the cybersecurity system at the European level was introduced with the EU Directive/2016/1148[135] , the so-called NIS (i.e., "*network and information security*") directive, which notably provided for the first mechanisms of strategic and operational cooperation between member states, certain obligations regarding security measures and incident notifications in key strategic sectors at the economic and societal levels.

Italy implemented the directive with Legislative Decree No. 65 of 2018. Much of the decree is dedicated to defining rules for internal coordination between administrations, identifying procedures for the future drafting of documents such as the National Cybersecurity Strategy, and establishing contact and cooperation points between different authorities. The approach has been criticized by some authors[136], the rules having very limited real impact on ICT practitioners.

On Nov. 10, 2022, the European Parliament approved the so-called "NIS2" Directive[137] having the primary purpose of expanding the scope of the previous so-called "NIS" Directive and preparing companies (both public and

---

[134] See Art. 1(3) of the regulation, which Stated, "*The objectives and tasks of the Agency leave without prejudice to the competencies of the member States with regard to network and information security that fall outside the scope of the EC Treaty, such as those covered by Titles V and VI of the Treaty on European Union, and in any case activities in the field of public security, defense, State security (including the economic well-being of the State where the issues relate to State security issues) and State activities in the field of criminal law.*"

[135] Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 on measures for a common high level of security of networks and information systems in the Union.

[136] B. BRUNO, cit., 14.

[137] Directive EU/2022/2555, entered into force on January 17, 2023.

private) for current and future cybersecurity challenges. Specifically, the NIS2 Directive provided for: (i) a substantial restatement and broadening of the scope of data security regulations; (ii) the strengthening of EU-level oversight bodies and activities, with the aim of improving collaboration to counter the global cyber threat by sharing experiences among member states; (iii) the streamlining of minimum security requirements and mandatory cyber incident notification procedures; and (iv) the extension of risk management and vulnerability assessment concepts to the entire supply chain, involving all or a greater number of stakeholders involved.

It should be noted that the NIS 2 Directive distinguishes between operators of "essential services" and "important services". The former category also includes public administrations, which are joined by operators in the energy, health, space, banking, transportation, digital infrastructure, electronic communications, and water sectors (see Art. 3(I)). "Important services" on the other hand, include operators of postal and courier services, waste management, the chemical sector, the agri-food sector, as well as the other services enumerated in Annexes I and II of the Directive and not included in the "essential services" category.

The Directive has the virtue of outlining (see Art. 7) the concept of a "*national cybersecurity strategy*", providing that Member States should establish, among other things, (i) a *governance framework for the* realization of objectives and priorities (see sub-paragraph (b)); (ii) a *governance* framework that clarifies the roles and responsibilities of relevant stakeholders at the national level (see (c)); (iii) identification of measures to ensure preparedness for and response to, and subsequent recovery from, incidents, including collaboration between the public and private sectors (see (e)); and

(iv) a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy (see (f)).

Of particular relevance for the present purposes is the second paragraph of Art. 7, where it is stipulated that as part of the national cybersecurity strategy, "*Member States shall in particular adopt policy measures regarding (a) cybersecurity in the supply chain of ICT products and services used by entities for the provision of their services; (b) the inclusion and definition of requirements regarding cybersecurity for ICT products and services in public procurement, including requirements regarding cybersecurity certification, encryption and the use of open source cybersecurity products*".

In other words, quite appropriately, cybersecurity becomes in the European framework a parameter for the awarding of public contracts concerning technological solutions for public administration. As will be seen *below*, Italy has not yet fully transposed the NIS 2 Directive, although it has included specific references to cybersecurity in the new public contracts code (Legislative Decree No. 23 of March 31, 2023).

Article 8 also stipulates that each Member State shall establish one or more competent authorities responsible for cybersecurity and the supervisory and sanctioning tasks regulated by Chapter VII of the Directive.

Finally, again for what is relevant to this contribution, it should be pointed out that the Directive provides in Article 24 that member states may require "essential" and "important" entities to use certain ICT products, ICT services, and ICT processes, whether developed by the "essential" or "important" entity or purchased from third parties, that are certified under the European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. In addition, member states encourage essential

and important entities to use qualified trust services. In other words, Member States are given the possibility to predefine upstream what are the essential characteristics of the technological solutions to be used for the performance of certain services pertaining to the most "sensitive" areas enucleated by the directive and mentioned above.

Subsequent Articles 31 to 36 also, while deferring to the member states for detailed regulations, give national competent authorities penetrating supervisory, control and sanctioning powers over both “essential” and “important” entities.

Having completed this dutiful reconstruction of the supranational discipline, it is necessary at this point to turn to the transposition discipline adopted at the national level.

Following the adoption of the Cybersecurity Act (EU Reg. No. 881/19) at the European level, at the national level, Decree Law No. 105 of 2019 was adopted on the “*Urgent provisions on the National Cybersecurity Perimeter*”. The decree law introduced into our legal system the institution of the Cyber National Security Perimeter (PSNC)[138] - while not providing a definition of it - referring to a decree of the President of the Council of Ministers modalities and procedural criteria for the identification of public administrations, entities and public and private operators, having a seat in the national territory, included in the cyber national security perimeter and required to comply with the measures and obligations provided by law.

[138] For a comprehensive analysis of the institution see, among others, B. CAROTTI, *Sicurezza cibernetica e Stato-nazione*, in *Giorn. Dir. Amm*., 5, p. 629; S. MELE, *Il perimetro di sicurezza nazionale cibernetica e il "nuovo" golden power*, in *Il diritto di internet nell'era digitale*, edited by S. PREVITI and G. CASSANO, Milan, Giuffré, p. 186. A. RENZI, *La sicurezza cibernetica: lo stato dell'arte*, in *Giorn. Dir. Amm.*, 4, 538.

Indeed, in implementation of the aforementioned decree, 3 Prime Ministerial Decrees and 1 Presidential Decree were adopted[139] .

Specifically, with the DPCM July 30, 2020, provisions were adopted regarding the identification of entities having the characteristics to be included in the National Cyber Security Perimeter. In particular, pursuant to Art. 3 of the aforementioned DPCM, for the purposes of inclusion in the Perimeter, reference must be made to entities operating in the government sector as well as "*additional entities, public or private, operating in the following sectors of activity: a) interior; b) defense;c) space and aerospace; d) energy; e) telecommunications; f) economy and finance; g)transportation; h) digital services; i) critical technologies, as referred to in Article 4(1)(b) of Regulation (EU) 2019/452 (...) l) social security/labor institutions*".

It appears evident, therefore, the care with which the legislature has enucleated the aforementioned areas, given the high level of technological "*pervasiveness*" (see *above*) that characterizes them. These areas are all intimately related to the provision of essential services, the performance of activities of general interest, and the protection of "sensitive" interests.

---

[139] (I) Prime Minister's Decree No. 131 of July 30, 2020 Regulations on national cybersecurity perimeter, pursuant to Article 1, paragraph 2, of Decree Law No. 105 of September 21, 2019, converted, with amendments, by Law No. 133 of November 18, 2019.

II) Presidential Decree No. 54 of February 5, 2021, "Regulations implementing Article 1, paragraph 6, of Decree Law No. 105 of September 21, 2019, converted, with amendments, by Law No. 133 of November 18, 2019."

III) Prime Minister's Decree No. 81 of April 14, 2021, "Regulations on notifications of incidents impacting IT networks, information systems and services referred to in Article 1, paragraph 2, letter b) of Decree-Law No. 105 of September 21, 2019, converted, with amendments, by Law No. 133 of November 18, 2019, and measures to ensure high levels of security."

IV) Decree-Law No. 82 of June 14, 2021 converted into Law No. 109 of August 4, 2021 on urgent provisions on cybersecurity, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency.

V) Decree of the President of the Council of Ministers June 15, 2021, - Identification of categories of ICT goods, systems and services to be used in the national cybersecurity perimeter, in implementation of Article 1, paragraph 6, letter a), of Decree-Law No. 105 of September 21, 2019, converted, with amendments, by Law No. 133 of November 18, 2019.

Subsequently, the Italian legislature, with the DPCM of June 15, 2021, after identifying the categories of "*subjects*" to be included in the Perimeter, enucleated the categories of "*ICT goods, systems and services*" intended to be used in the national cybersecurity perimeter, such as (i) hardware and software components that perform telecommunication network functionalities and services; (ii) hardware and software components that perform functionality for the security of telecommunications networks and the data they process; (iii) hardware and software components for data acquisition, monitoring, supervisory control implementation and automation of telecommunications networks and industrial and infrastructure systems; and (v) software applications for the implementation of security mechanisms.

In light of this, subsequently, by a separate administrative act of the Prime Minister's Office not subject to publication (but rather exclusive communication to those directly concerned), the subjects included in the Perimeter were concretely identified. This administrative act is subtracted from access, in line with the purpose of protecting national security underlying the creation of the Perimeter, thus falling under this limitation among those provided for in Article 24, Law No. 241/90.

At this point, it is intended to briefly review the burdens and responsibilities of an entity included in the Perimeter, focusing only on those deemed useful in the economy of this paper[140].

Once included in the perimeter, the entity-which, it is reiterated, can be a PA or a public or private operator with "*an establishment in the national territory*" and on which depends the exercise of an essential function of the

[140] On the topic see A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, in *Giorn. dir. amm*., no. 4, 2021, 546 ff; S. Mele, *Il Perimetro di Sicurezza Nazionale Cibernetica e il nuovo "golden power"*, in G. CASSANO-S. PREVITI, *Il diritto di internet nell'era digitale*, Milan, Giuffré, 2020, 186.

state or "*the provision of a service essential for the maintenance of civil, social or economic activities fundamental to the interests of the state*" - has rather stringent obligations.

First, there is a requirement to notify the Computer Security Incident Response Team (CSIRT) of any incidents impacting networks, information systems and IT services. Notification must be completed within a variable period of one hour or six hours in the case of incidents involving ICT assets included in the list in Annex A of Presidential Decree No. 81 of April 14, 2021. Specifically, notification must be made within six hours of discovery in cases of breach or loss of confidentiality or integrity, access via malware, lateral movement, or data collection and exfiltration actions. This time window is reduced to one hour from discovery, in cases of inhibition of response functions, compromise of control processes, disruption or breach of services, systems or data.

The deadline to proceed with the incident notification is extended to 72 hours in case of incidents impacting assets other than those included in the list of ICT assets prepared by the subject. The incidents subject to notification, consist, among others, of 'unauthorized access, execution and installation, lateral movements, exfiltration of information and data, reconnaissance referred to spearphishing activities, which go to impact assets that are outside the Perimeter and for this reason considered less at risk, but which could have a subsequent negative effect on ICT assets of assets belonging to the same supply-chain.

It should be emphasized for the purposes of this writing that if an entity included in the Perimeter intends to proceed with the awarding of contracts for the provision of ICT goods, systems or services for use on networks, information systems and for the performance of IT services, it must notify the

Center for National Evaluation and Verification (CVCN), established at the Agency for National Cybersecurity (ACN), which (as it will elaborate further *below*) may require the inclusion in calls for tenders and contracts of clauses, including suspensive or termination clauses, aimed at complying with any conditions and tests ordered by the CVCN.

Entities included in the Perimeter are also obliged to prepare the list of ICT assets of their respective relevance, indicating their component networks, information systems and IT services (D.P.C.M. July 30, 2020 No. 131 "Regulations on the National Cybersecurity Perimeter").

In this context, with Decree Law No. 82 of 2021, the legislature defined the national *governance* of the cybersecurity system[141] , with the President of the Council of Ministers at its top, who has the overall direction and responsibility for cyber security policies, including the adoption of the national strategy and the appointment of the top management of the new National Cybersecurity Agency. The latter, was precisely established in transposition of the NIS Directive, with accounting, organizational and financial autonomy, following the typical traits of administrative agencies, where technical and specialized functions converge with the needs of political direction and control related to such a sensitive area[142] . It, in fact, performs technical functions aimed at protecting national interests in the field of cybersecurity. However, the high technical expertise typical of the sector and the need to ensure a certain independence from political power, due to possible friction with the guarantee of fundamental rights and freedoms, led the legislature to grant the Agency "*a*

[141] I. FORGIONE, cit., 1116.

[142] On the figure of the Agency see, *ex plurimis,* G. ARENA, *Agenzia amministrativa,* in *Enc. Giur. Treccani*, Roma, 1999; C. FRANCHINI, *L'organizzazione*, in S. Cassese (ed.), *Trattato di diritto amministrativo*, I, Milano, Giuffré,2003, 297 ff.

more pronounced autonomy from other agencies" thus placing it "*outside the agency model created by Legislative Decree No.* 300/1999"[143] .

With reference to the functions carried out by the Agency, it must be highlighted that it is mainly attributed with tasks pertaining to the prevention and protection of national security in cyberspace, inspection, assessment and imposition of prescribed sanctions in case of violation of sector regulations[144] , management of cyber vulnerabilities and law enforcement activities in case of attack. Within these latter activities, functions of great importance are attributed to CSIRT Italy, introduced when the NIS directive was transposed and hinged, at first, at the DIS and, today, transferred to the Agency. It is the responsibility of the aforementioned intervention group, in particular, to periodically monitor the occurrence of attacks and incidents at the national level, to receive mandatory reports from operators and optional reports from other entities, public and private, otherwise affected by a cyber threat, to issue pre-alerts and alerts and to offer operational assistance in crisis situations.

Well, according to some authors[145] , the establishment of the authority, which operates as a single interlocutor for the entities included in the Cybersecurity National Security Perimeter, appears to lend greater compactness to a regulatory design that was initially fragmented and complex,

---

[143] F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi*, 12/2022, 249 and the Dossier on "*Urgent Provisions on Cybersecurity, Defining the National Cybersecurity Architecture and Establishing the National Cybersecurity Agency*" of July 23, 2021, available at https://temi.camera.it/leg19/dossier/OCD18-15472/disposizioni-urgenti-materia-cybersicurezza-definizione-architettura-nazionale-cybersicurezza-e-istituzione-agenzia-cybersicurezza.html.

[144] Specifically, the National Agency is responsible for the assessment and imposition of administrative sanctions provided for in Legislative Decree No. 65/2018, on the subject of network and information system security, EU Reg. 2021/887 and Legislative Decree No. 123, on the subject of cybersecurity certification system, by d.l. no. 105/2019, on the subject of National Cybersecurity Perimeter, and by d.lgs. no. 259, August 1, 2003 (so-called Electronic Communications Code), on the subject of protection of publicly accessible electronic communications networks and services.

[145] L. PREVITI, *Pubblici poreri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi*, no. 25/2022, 80.

which is now marked by the centralization of competencies and the coordination of strategic lines and operational actions, with a view to simplifying decision-making procedures and eliminating pre-existing functional overlaps[146] .

That dutiful reconstruction of the cybersecurity system in our system having been completed, it is now necessary to turn to an examination of the ways in which the latter and the paradigm of public contracts are integrated, in order to highlight the mutual influences of the two spheres, especially in light of the new Code[147] . As it will be noted, we anticipate, the discipline on public contracts sins by a substantially generalized lack of coordination with that cybersecurity described above, despite the fact that public evidence procedures (understood in a broad sense) are the most widely used procurement model available to the P.A. for the provision of the technological solutions they need.

4. Cybersecurity as award criteria: lights and shadows of the changes brought by the new Public Procurement Code

As anticipated, given the pervasiveness and centrality of technological solutions offered by private economic operators to address the digital transition process of the Public Administration, the issue of cybersecurity of digital infrastructures appears increasingly central. The acquisition of the aforementioned solutions by the Administrations inevitably passes through the public evidence model, except in the case of contracts - on which we cannot

[146] As lucidly pointed out in M. MATASSA, *La regolazione della cybersecurity in Italia*, in *La sicurezza nel cyberspazio*, edited by R. URSI, Franco Angeli, Milan, 2023, p. 36, "*the overall design of the new architecture sees the specialist structures recalled operate in synergy with other traditional administrations that are assigned exclusive prerogatives reconnected to their institutional mandate. In this context, the intelligence branch (and in particular the DIS) is called upon to provide the ACN with a useful information framework to progressively guide the measures aimed at ensuring the proper implementation of the plan; the Ministry of the Interior carries out activities to prevent and counter cybercrimes as the national public security authority; and, finally, the Ministry of Defense performs functions of coordination of military policy, governance and military capabilities in the cyber environment.*"

[147] Legislative Decree No. 36 of March 31, 2023.

dwell here - secreted[148] or tendered directly by the National Cybersecurity Agency[149] .

In this regard, it is interesting to note that the Italian legislature introduced the concept of cybersecurity in the new Public Contracts Code (Legislative Decree No. 36 of March 31, 2023), where any reference to cybersecurity was instead absent in the previous version of the Code recited by Legislative Decree No. 50 of April 18, 2016. Specifically, the reference to cybersecurity was included among the criteria for the awarding of tender procedures. Specifically, Article 108 (headed "*criteria for the award of works, services and supply contracts*") in Paragraph 4 stipulates that contracting stations in the evaluation of the technical elements of the bids of competitors[150] shall always take into account cybersecurity elements in the procurement of IT goods and services, particularly when the use of such goods and services is found to be "*related to the protection of strategic national interests*".

The downfall of such a provision is that contracting stations will be required to value such aspects in order to identify the best value for money and ensure "*effective competitive comparison on technical profiles*," including "*cybersecurity elements*," paying special attention in cases where the use of the goods or tools is related to the protection of strategic national interests. Furthermore, in these cases, the same legislator has established that the contracting station must decree a ceiling for the economic score within the limit of 10 percent, with a consequent preponderant enhancement of the technical component when evaluating bids (especially compared to the model

[148] Regulated by, among others, Article 139 of Legislative Decree No. 36 of March 31, 2023, and Article 42 of Law No. 124 of August 3, 2007. In doctrine, see D. SABATINO, *Contratti della difesa e contratti secretati*, in *Trattato sui contratti pubblici*, edited by M.A. SANDULLI and R. DE NICTOLIS, Milan, Giuffré, 2019, IV, 923 ff.

[149] Regulated by DPCM September 1, 2022, No. 166.

[150] In cases where the criterion of the most economically advantageous tender is applied.

recited in the previous Code, where it was provided as a general rule, in paragraph 10-bis of Art. 95, that the economic component could weigh no more than 30 percent[151]), such that it would result in a lower impact of the price component, which would be less decisive in the face of other factors related to cybersecurity and digital security.

With reference to the objective scope of the provision, it seems reasonable to assume that it does not apply only to supplies involving devices aimed at ensuring the cybersecurity of public digital infrastructure, but in general to all procurements aimed at the procurement of IT goods and services, as long as they consume "*the protection of* strategic *national interests*".[152]

The provision (introduced in Parliament, where the draft prepared by the Special Commission established at the Council of State had made no reference to it)[153] , while having the virtue of introducing (finally) the parameter of

[151] On the inclusion of such an abstract, predetermined and mandatory limit, the doctrine had from the outset raised doubts of European compatibility, theoretically extendable also to the new wording of Article 108. On this point, see F. CARDARELLI, *Criteri di aggiudicazione*, in *Trattato sui Contratti Pubblici*, edited by M.A. SANDULLI and R. DE NICTOLIS, Milan, Giuffré,2019, 564.

[152] The concept suffers from a not indifferent generality, so much so that already from the first applications the central purchasing agency Consip excluded the strategic relevance of some procedures, in order to exclude the applicability of paragraph 4 of art. 108 of the new Code. In reference is to the "*Open procedure for the awarding of framework agreements concerning application services in clpud optics and demand and pmo services for local public administrations - ID 2610*". Specifically, in the preamble to the Terms of Reference (p. 5), although this is a procedure for the nationwide provision of IT services, it is clarified that "*this initiative does not apply to cybersecurity regulations since the contract is for ICT services that are not strictly related to those identified by the DPCM of June 15, 2021, published on August 19, 2021. Contracting administrations will not be able to use this initiative for the procurement of services falling under employment contexts "related to the protection of strategic national interests," pursuant to Article 108, paragraph 4, of the Code.*"

[153] It seems reasonable to believe that the integration is the result of the indications provided by the National Cybersecurity Authority in a parliamentary hearing (document available at the following link: lhttps://documenti.camera.it/leg19/documentiAcquisiti/COM08/Audizioni/leg19.com08.Audizioni.Memoria.PUBBLICO.ideGes.7977.15-06-2023-15-03-25.709.pdf) according to which "*in view of the complexity of the field of cybersecurity and digital more generally, one could, likewise, reason about the criterion for awarding contracts when using that of the economically most advantageous offer. (...) it seems of all importance, therefore, that the contracting station give appropriate weight to the technical-quality profiles of cybersecurity over the economic profiles, not being able to risk the price element being decisive, even through tender mechanisms that recognize the necessary attention that contracting stations must have for these aspects*."

cybersecurity within the discipline of public contracts[154] , nevertheless has several critical issues.

First, it seems reasonable to ask whether it is correct (and, above all, exhaustive) to attribute to the respect of cybersecurity elements the value of a "mere" awarding criterion and not also a necessary requirement for participation (on this second profile, see *below*). The criterion of the economically most advantageous offer (where the provision under comment is grafted) is the result of the evaluation of quantitative (price, time of execution...) or qualitative (aesthetic and functional characteristics, quality, technical merit...) elements inherent to the nature and object of the contract, chosen by the contracting authority and explained in the tender *lex specialis*, to which the same contracting authority assigns "weights" that represent the usefulness of the individual element with respect to the overall result pursued through the contract[155].

From this perspective, contracting stations have a certain margin of discretion both in choosing the elements to be evaluated and in determining the extent of their importance, it being up to them to establish the criteria and/or sub-criteria for the comparative evaluation of bids, as well as the related scores or sub-points, evidently within the limits of proportionality and reasonableness with respect to the specificity of the contract[156].

---

[154] The new Code also deals with the issue of security in Article 19, paragraph 5, where it States that those involved in the digitized contract lifecycle "*shall take technical and organizational measures to safeguard IT security and personal data protection.*"

[155] Thus F. CARDARELLI, *Criteri di aggiudicazione*, in *Trattato sui Contratti Pubblici*, *cit.*, 560; ANAC Guidelines No. 2. On the issue of OEPV in light of the new Code, see M. MIRRIONE, *La selezione delle offerte*, in *Il nuovo corso dei contratti pubblici. Principi e regole in cerca di ordine*, edited by S. FANTINI and H. SIMONETTI, Il Foro Italiano-Gli speciali, 2023, no. 1, 146 ff.

[156] On this point*, ex plurimis,* Cons. St., Sec. V, June 7, 2021, no. 4301, but also F. CARDARELLI, *Criteri di aggiudicazione*, in *Trattato sui Contratti Pubblici*, *cit.*, 561.

Well, the aforementioned margins of discretion appear particularly pronounced in the provision under comment, where the contracting stations are given the power to attribute, in the evaluation of the qualitative elements of the bids pertaining to the procurement of IT goods and services - "*specific and peculiar prominence*" in the enhancement of "*cybersecurity elements.*" The *rationale of* the provision is evidently to reward companies that are *compliance* with the cybersecurity requirements demanded in the procurement of technological solutions for the public administration, and undoubtedly, it must be viewed favorably, expressing a new sensitivity of the legislature on these issues. However, since the provision applies, as mentioned above, to procurements related to "*the protection of strategic national interests,*" it is not clear why no reference was made to the recalled architecture of the National Cybersecurity Perimeter, *ipso iure* applicable to this type of procurement, and which should therefore have been recalled. The application of that framework, moreover, as will be better seen in the following section, elevates compliance with cybersecurity *standards* from an award criterion to a participation requirement. This is because the awarding of contracts pertaining to the Perimeter can almost exclusively concern "certified" services, where compliance with cybersecurity elements is not a mere circumstance to be "rewarded" but more precisely a *conditio sine qua non* for taking part in the procedure. A circumstance, the latter, obliterated by the new Code.

Moreover, the same cited second paragraph of Art. 7 of the NIS II Directive, as noted above, provided that as part of the national cybersecurity strategy, "*Member States shall in particular adopt policy measures regarding: a) cybersecurity in the supply chain of ICT products and services used by entities for the provision of their services; b) the inclusion and definition of requirements regarding cybersecurity for ICT products and services in public*

procurement, including requirements regarding cybersecurity certification, encryption and the use of open source cybersecurity products".

The lack of coordination between Article 108 and the aforementioned national and supranational cybersecurity legislation is likely to generate doubts and uncertainties in its application, to the detriment of companies operating in the described sectors.

These critical issues, in addition to those generated by the lack of coordination, appear all the more accentuated if one considers the high margin of discretion that the provision gives to contracting stations in the evaluation of the qualitative elements of technical bids in the contracts described. Although it is among the shared prerogatives of the new Code to leave contracting stations greater margins of discretion in the awarding of public contracts[157] , in the case of Article 108, paragraph 4, there is a risk of trespassing into a kind of arbitrariness conferred on contracting stations, lacking at all the coordinates for the exercise of discretionary power. Reference is made generically to the concepts of "*cybersecurity elements*" and their "*enhancement*" lending themselves, however, to a myriad of different declinations of these indeterminate concepts. Indeed, of the two, one is either intended to refer to the cybersecurity certifications and *standards* that must be possessed and adhered to by the technological solutions provided to P.A. in the light of the regulatory framework of reference (see *above*), but in that case, rather than rewarding elements to be "evaluated", it should more correctly

[157] On this point, among others, F. CINTIOLI, *Il principio di risultato nel nuovo codice dei contratti pubblici*, in www.giustizia-amministrativa.it; L. CARBONE, *La scommessa del codice dei contratti pubblici e il suo futuro*, in www.giustizia -amministrativa.it; S. PERONGINI, *Il principio del risultato e il principio di concorrenza*, in Dir. e soc, 2022, 3, 551 ff.; M.R. SPASIANO, *Principi e discrezionalità nel nuovo codice dei contratti pubblici*: *primi tentativi di parametrazione del sindacato*., in federalismi.it, 2023, no. 24, 222 ff.; as well With regard to the Outline of the Code see M.A. SANDULLI, *Prime considerazioni sullo scema del nuovo codice dei contratti pubblici*, in Giustiziainsieme.it, December 21, 2022.

speak of requirements to be "ascertained" for the purposes of participation in the tender; or, alternatively, if it is intended to refer to the generic compliance of the technological solutions provided with the general canons of cybersecurity, the provision appears excessively vague and risks giving contracting stations the power to excessively or unbalanced enhancement of these profiles.

This last critical issue appears even more evident if one imagines the inevitably reduced competence of the administration with reference to *cyber* profiles, especially from a technical point of view. Really one struggles, therefore, to imagine a proper *ex ante* parameterization of the scoring criteria with reference to these aspects. According to some authors, a hermeneutic parameter may be represented by the definition of cybersecurity inferable from Decree-Law No. 82/2021, which refers to the "*set of activities (...) and obligations arising from international treaties, necessary to protect from cyber threats networks, information systems, computer services and elletronic communications, ensuring their availability, confidentiality and integrity by guaranteeing their resilience, including for the purpose of protecting national security and the national interest of* cyberspace"[158] . The reference, in any case, does not fully clarify what the "*cybersecurity elements"* might be that the legislature believes should be emphasized in scoring.

In essence, as anticipated by some early commentators, the provision is "*insufficient in terms of* content"[159] such that it necessarily needs to be supplemented taking into account the other relevant provisions on the subject, in order to prevent the discretion of contracting stations from encroaching on

[158] C. CATARISANO, *Commento sub. Art.* 108, in *Codice dei contratti pubblici annotato*, edited by L.R. PERFETTI, 829.

[159] Thus S. ROSSA, *Cybersecurity e pubblica amministrazione,* cit., 133.

mere arbitrary exercise of public powers capable of generating uncertainty and potential unequal treatment among economic operators.

A possible element of mitigation of this risky drift appears with all evidence to be constituted by Article 93, paragraph 2, of the Code, where it is specified that "*the commission shall be composed of an odd number of members, in a maximum number of five, experts in the specific sector to which the object of the contract refers.*" While the provision is purely programmatic in nature, it should theoretically enable the formation of qualified selection commissions capable of interpreting the needs of the contracting stations with sufficient punctuality and, to the effect, feed the latter into the scoring criteria. The provision, moreover, must also be read in light of art. 62 of the new Code, where aggregation and centralization of purchasing are regulated, institutes that pursue the primary purpose of ensuring that contracts above a certain threshold of relevance are managed and awarded only by "qualified" contracting stations or central purchasing bodies (such as, among others, Consip). A regulatory arrangement that clearly pursues the aim of ensuring, in contracts of a certain importance, skills as high as possible as well as proportionate to the value and strategic nature of the orders to be entrusted[160].

5. Compliance with cybersecurity *standards* as a substantial market access criterion

As anticipated, although not expressly stated within the Public Contracts Code, compliance with cybersecurity *standards* constitutes in some cases, *de facto*, a prerequisite for access to tenders and consequently to the ICT public procurement market, especially if the object of the supply are technological

[160] On this topic see G. FONDERICO, *I soggetti: stazioni appaltanti e operatori economici*, in *Il nuovo corso dei contratti pubblici. Principi e regole in cerca di ordine*, edited by S. FANTINI and H. SIMONETTI, Milan, La Tribuna, 77 ff.

solutions for which it is necessary to possess a certain certification attesting *compliance* with the requirements sanctioned at the European level[161] .

The compliance with the crises imposed by cybersecurity regulations becomes a requirement for access to tenders (as we have seen, in the Italian example it entails inclusion in the National Cybersecurity Perimeter), a requirement that can be detailed by national authorities (CVCN) that also have the power to modify and/or supplement calls for tenders. The combination of these elements results in a considerable filter of access to the market for public contracts in technology, with significant consequences in competitive terms that cannot be ignored.

As mentioned, Decree Law No. 105 of 2019 has given the Center for National Evaluation and Certification (CVCN), now established at the National Cybersecurity Agency, a rather peculiar role that pertains to the verification on the *procurement* of entities included within the Cybersecurity Perimeter or the central purchasing bodies to which they resort[162] . Indeed, these entities, pursuant to Article 1, paragraph 6, of Decree Law No. 105/2019, if they intend to proceed with the procurement of ICT systems and services that are intended to be used on the networks, information systems and for the performance of IT services included in the Perimeter have the obligation to notify the CVCN of this intention, together with the risk assessment[163] associated with the object of the supply, including in relation to the scope of

---

[161] In this regard, as lucidly observed in S. Rossa, *Cybersecurity and e pubblica amministrazione,* cit., 160, "*both the imposition of technical standards and ad hoc cyber-organizational measures, as well as the obligation to adopt a common minimum cyber certification framework for goods, services or systems, could actually be useful in preventing situations that could lead to cyber risks. On closer inspection, however, the two mentioned obligations allow the goal of making networks and digital infrastructures cyber-safe to be achieved only in the very short term, that is, as long as the technological level of attackers is equal to that of the institutions, to whose technical specifications the regulations refer. I...I The danger, therefore, is that by the time these obligations are to be implemented the technological context of reference will have changed such that such impositions will be ineffective (...).*"

[162] For a careful reconstruction see S. ROSSA, *Cybersecurity e pubblica amministrazione,* cit., 155 ff.

[163] L. PREVITI, cit., *passim*.

use. From the receipt of the communication, the CVCN has a period of 60 days (extendable once) to carry out preliminary verifications and, if necessary, also impose conditions and tests of hardware and software to be carried out also in collaboration with the entities (public or private) making the communication[164] . After the tests have been carried out, the CVCN can determine with a measure of acceptance (with or without prescriptions) or denial (thus inhibiting the conduct of the bidding process with adequate justification).

Well, the exercise of such powers poses some orders of problems.

First, it is not clear from reading the regulations whether the verifications of the CVCN, which enjoys very broad technical discretion[165] , should be conducted before the public tender is held or after the award. Theoretically, it would be more appropriate to conduct such verifications upstream. However, the need for tests to be carried out on the technologies to be installed implies that these have already been identified even though this would be poorly reconciled with the principle of good performance as well as the principle of results, since in the event of negative outputs by the CVCN with respect to the identified technological solution, there would be a risk of nullifying the procedure.

Moreover, the same Art. 1 of the aforementioned Decree-Law No. 105 provides that in the event that the CVCN needs tests or verifications on software, it may be "*supplemented the invitations to tender and the related contracts with clauses that condition, suspensively or resolutively, the contract on compliance with the conditions and the favorable outcome of the tests.*" Such a provision as lucidly observed in doctrine[166] , clashes with the

[164] Detailed regulations regarding the mechanism of assessment tests as well as the CVCN's powers of verification and inspection were introduced by Presidential Decree No. 54 of February 5, 2021.

[165] S. ROSSA, *Cybersecurity e pubblica amministrazione,* cit., 162.

[166] B. BRUNO, cit., 31.

fundamental European and national principles of *favor partecipationis*, transparency and *par condicio*, under which a heterointegration of the *lex specialis* during the tender process, especially if left to administrative evaluations carried out *ex post,* could hardly be admitted. Emblematic in this sense would be the case in which the CVCN considered it necessary to possess certain technical requirements that were not provided for in the tender *lex specialis* and on the basis of which the economic operators had bound themselves to submit bids.

For these reasons, the most reasonable hypothesis would seem to be that of the upstream involvement of the CVCN, with a careful analysis of the needs of the public administration as well as the call for tenders and further documentation, in order to establish with certainty and in advance the requirements for participation in the public tender in order to avoid "surprises" for competing economic operators. Requirements that, moreover, if deemed excessively strict or preclusive of participation by economic operators could be challenged before the administrative judge.

Not secondary in this respect appears to be the issue of the costs to be incurred for any tests prescribed by the CVCN, which, pursuant to Article 9 of the aforementioned Presidential Decree No. 54 of February 5, 2021, are entirely borne by the supplier. These costs, as is evident, can be really considerable and being uncertain it is not clear how they can be quantified in advance by the economic operator when formulating the offer. This aspect entails, in essence, at least two critical issues: i) first, there is a risk of violating the principle of immodifiability of the offer, where the economic operator would be allowed to modify its economic proposal during the course of the tender; ii) under concurrent profile, where such modification would not be

allowed, there would be a risk of completely eroding the profit budgeted by the economic operator so as to irreparably alter the contractual synallagma[167] .

The barrier posed to entry into the public contracting market by the high technical standards required, moreover, entails significant problems from a competitive point of view. This is because, as is evident, inclusion (or not) in the National Perimeter may result in the survival (or not) of a company operating in the IT services sector given the economic significance of public contracts.

In this regard, it should be pointed out that recital 74 of Directive 2014/24/EU on public procurement provides for that "*technical specifications set by public procurers must allow public procurement to be opened up to competition as well as the achievement of sustainability objectives. To this end, it should be possible to submit bids that reflect the variety of technical solutions, standards and technical specifications prevailing on the market, including those defined on the basis of performance criteria related to the life cycle and sustainability of the production process of works, supplies and services. (...) Accordingly, technical specifications should be drafted in such a way as to avoid artificially restricting competition through requirements that favor a specific economic operator by reflecting the main characteristics of the supplies, services or works it usually offers*". In the same sense, Article 42(2) of the Directive expressly provides for that "*technical specifications shall afford equal access of economic operators to the award procedure and not*

[167] Emblematic in this sense is the answer to question no. 38 issued by Consip on the occasion of the tender for the award of the supply of server technologies and related and optional services for public administrations (4 Edition - ID 2383) according to which "*In the case of activation of preliminary verifications and/or imposition of conditions and hardware and software tests on the supplies covered by this agreement, referred to in Law no. 133/2019, as well as indicated in paragraph 10 of Article 3 of the recalled outline of the agreement, having the same suspensive or resolutive character of the supply order, should the supplier be involved in the performance of said activities, the related costs must be considered to be borne by the supplier itself limited to the areas of specific competence.*"

involve the creation of unjustified obstacles to the opening-up of public procurement to competition".

Because of this, it is absolutely essential that public administrations, in consultation with the CVCN, in concretely implementing the European provisions that identify the requirements for access to the National Perimeter, do not run the risk of artificially altering the competitive ICT services market game by placing barriers to entry that are difficult to cross. The whole, moreover, suffers from a lack of rationality in the entire legal framework of reference, which does not allow economic operators to assess with certainty, ex ante, which *standards* they are required to meet and which certifications to possess in order to be sure of accessing the public procurement market in the sector *de quo*.

Well, beyond the literal scope of the provisions, which, as we have seen, could lead to difficulties of no small moment in the application phase, it is essential that the burdens placed on economic operators, in addition to being predeterminable, are respectful of the principle of proportionality[168] , without risking leading to a heterogenesis of ends. In this regard, the role played by the National Cybersecurity Authority will be decisive, which will have to supervise the concrete application of the regulatory apparatus of reference, apply sanctions in case of violations and, where necessary, participate in the implementation of the regulatory framework in consultation with the Presidency of the Council of Ministers. In this context, the difficult balancing act between the interest in the security and "resilience" of the technological infrastructure of the public administration, on the one hand, and that of the

[168] On the application of the principle of proportionality see D.U. GALETTA, *Il principio di proporzionalità*, in M.A. SANDULLI, *Codice dell'Azione Amministrativa*, Milan, Giuffré, 2017, 149 ff.

freedom of private economic initiative as well as free competition, on the other, will have to continue to be accomplished.

6. First concluding remarks

In light of the analysis conducted let some initial insights be allowed.

In the outlined context of rapid evolution, where the actors and interests at stake are changing, it seems crucial to think about the possible reorganization of the reference discipline as well as a greater enhancement of cooperation between public and private actors.

As we have seen, the dialectic between public and private actors is as peculiar as ever in the area covered by the present analysis: the State invests in innovation to stimulate the development of new technological solutions, arriving at being considered as itself as an "innovator" subject[169]; the State in turn is the first user of the aforementioned solutions, which inevitably accompany the public administration in the process of digital transition; in turn, both public and private actors involved in the digital innovation of public infrastructure actively participate in the implementation of the cyber defense strategy.

In such a scenario, the regulations on the awarding of public contracts (*i.e.,* of the rules of the game) must be clear and guarantee *ex ante* knowability of the conditions for access to the market. Only in this way, indeed, can the proper fulfillment of the ongoing digital transition process be guaranteed, allowing private companies to approach the public contract market having full knowledge of the necessary requirements for participation in tenders, as well as of "whether" and "how" the elements pertaining to the cybersecurity profile will be considered when evaluating the offer. After all, as is well known, a

[169] M. MAZZUCCATO, *Lo Stato innovatore*, Bari, 2014.

condition of legal uncertainty can only negatively impact a country's growth, market performance[170] as well as, in this case, the phenomenon of digital transition of public administrations.

Under concurrent profile, it is agreed with those who believe that the phenomenon of cybersecurity of public digital infrastructures should also be inspired by a "collaborative-oriented" relationship between public and private entities,[171] into which must be grafted a profound process of training and awareness-raising of public officials on the subject, as well as an involvement of private parties in the refinement of regulation (perhaps through a dialogue on the model of *notice and comment* with the National Cybersecurity Authority). This would make it possible to mitigate the critical issues arising from information asymmetry and the phenomenon of so-called *lock-in*, freeing

---

[170] On the topic, among all, see M.A. SANDULLI, *Il ruolo dei principi nel diritto amministrativo. Introduzione a Principi e Regole dell'azione amministrativa – Quarta Edizione 2023*, in www.giustiziainsieme.it where the author lucidly elucidates that "*In a constitutional State of law, the power to authoritatively interfere in the legal sphere of others must evidently be defined and delimited by a clear and certain normative context (principle of legal certainty, declined in the principle of legality), i.e., by prior legal rules, general and abstract, more or less stringent (to which corresponds the graduation of administrative power from binding to discretionary (on which see the appropriate contribution immediately below), of a substantive (fixing of objectives to respond to specific public interest finalities) and procedural (competence, mode and timing of action, effects, etc.), which ensure the impartiality of public action ...) and the best balance of the various interests (public and private) involved (principle of good administration ...).Compliance with these rules must, moreover, be ensured through appropriate systems of control (internal and external) and, above all, through adequate modes of judicial protection (principle of effectiveness of protection), which, tendentially, justify a special system of administrative justice (which may or may not provide for the establishment of a judicial apparatus different and autonomous from the ordinary one).*" On this topic, see also F. ZACCARIA, *La perdita della certezza del diritto: riflessi sugli equilibri dell'economia e della finanza pubblica*, Pavia, 2003; C. MIRABELLI, *Il rischio da diritto. Il costo dell'incertezza ed alcune possibili economie*, in *La certezza del diritto - Un valore da ritrovare - Atti del convegno*, Firenze, 2-3 ottobre 1992, Milano, 1994, 39.

[171] S. ROSSA, *Cybersecurity e pubblica amministrazione,* cit., 221. In the same vein, the document bearing the "National Cybersecurity Strategy," published by the Italian Council Presidency in May 2022, States that transversal to the objectives of the strategy is the public-private partnership, marked by "*a whole-of-society approach, which sees the public sector acting synergistically with the private sector, academia and research, the media, families and individuals to strengthen the cyber resilience of the nation and society as a whole. The cyber space, moreover, consists of ICT products and services made or delivered mainly by private entities. For this reason, the present strategy cannot disregard full collaboration and constant public-private consultation, (...).*" On this point also L. PREVITI, *La collaborazione pubblico-privato nel sistema multilivello di sicurezza cibernetica*, in *La sicurezza nel cyberspazio*, edited by R. URSI, Franco Angeli, Milan, 2023, p. 157, where the author examines the current national legal context highlighting all its limitations with respect to an effective collaborative dynamic between public and private subjects.

public administrations from the state of constant subordination to large companies supplying technological solutions, allowing for the effect that the same contracting stations can strategically orient their purchasing needs and more knowledgeably prefix both the access requirements and the award criteria.

In this context, echoing the insights anticipated in the opening, the role of the state is thus evolving. The public and private spheres find themselves sharing the same challenge of countering cyber threats, albeit from different angles. Therefore, it no longer makes sense to think of the legal experience within the opposition between public and private, and it is rather necessary to replace it with a new paradigm, characterized by "*interchangeability of roles, modification of relationships, and trade in rules and* ordering *principles*"[172] The current landscape, in conclusion, calls for a reprioritization and a more forward-looking role of the state is required, capable of outlining national strategies aimed at cyber defense as well as strengthening the rules of public evidence for technology procurement, with the aim of strengthening organizational resilience in the different domains, all with increasingly close cooperation between the public and private sectors.

[172] S. CASSESE, *L'Arena pubblica. Nuovi paradigmi per lo Stato*, in *Riv. trim. dir. pubbl.,* 3, 2001, p. 601.

CHAPTER III

PUBLIC PROCUREMENT FOR THE PROVISION OF TECHNOLOGY SOLUTIONS. TRANSPARENCY AND COMMERCIAL SECRECY

SUMMARY: 1. Introduction. 2. Public Procurement as “tool” and “purpose” of the digital transition. 3. Algorithmic "opacity" between the principle of transparency, the right to good administration, trade secrets and intellectual property. Perspectives *de iure condito* in the light of the European legal context. 4. Perspectives *de jure condendo* in the light of the proposed regulation on AI. 5. First concluding remarks.

1. Introduction

Over the last twenty years, technology has taken an increasingly central role in people's existence. This has led to a rise in the quality of life of the community thanks to a phenomenon of massive 'delegation' to new technologies of complex and time-consuming tasks and duties, reaching in some cases, indeed increasingly frequent, a veritable substitution of the human being.

This process, albeit with a physiological delay of a few years, is inevitably also affecting the public administration, leading some authoritative scholars to speak of "Public Administration 4.0."[173] . Indeed, innovation in the public sector is a crucial junction for the development of States, which invest considerable resources in this field. This is also confirmed by the expenditure

[173] D.U.GALETTA-J.G. CORVALÀN, *Intelligenza artificiale per una pubblica amministrazione 4.0?*, cit., in *Federalismi*, no. 3/2019.

items of the Next Generation EU, where a significant portion of investments is dedicated to the digital transition of public administrations[174] .

Moreover, Europe has long since launched a project for a common strategy on technological innovation, aware of the need for a common approach among all Member States, especially in an area where territorial boundaries appear blurred.

The "digital transition" of the public administration, as clarified by authoritative scholars[175], implies the use of information and communication technologies (ICT) within the public sector, with the aim of delivering services that meet the needs of citizens, in a social context that has radically changed thanks to the use of these technologies[176]. In other words, action must be taken on the technological innovation of public infrastructures in order to deliver better services, in less time and with significant cost savings in the long run[177] . Well, the innovation of public administration must not be conceived as such, but rather instrumentally in the pursuit of the public interest prefixed *ex ante*.

In order to live up to the needs of the community, the digital transition process must inevitably take the form of the administration's use of artificial intelligence systems, software, data computing and blockchain platforms. In most cases, administrations do not have the necessary expertise in-house to

[174] Significantly, in the Italian Plan (PNRR) 27% of resources are dedicated to digital transition.

[175] D.U. GALETTA, *Transizione digitale e diritto ad una buona amministrazione, cit.*, in *Federalismi*, no. 7/2022, p. 104; Id., *Information and Communication Technology an d Public Administration: through the Looking Glass*, in D.U. GALETTA-J. ZILLER (Eds.), *Information and Communication Technologies Challenging Public Law*, *beyond Data Protection*, Nomos Verlagsgesellschaft, 2018, p. 119 ff.

[176] Z. ENGIN-P. TRELEAVEN, *Algorithmic Governance: Automating Public Services and Supporting Civil Servants in using Data Science Technologies*, in *The Computer Journal*, Vol. 62, No. 3, 2019; T. AHMED, *GovTech: An Emerging Sector Revolutionising Public Services*, in www.govtechresearch.com.

[177] P. CERQUEIRA GOMES, *EU Public Procurement and innovation*, Cheltenham, 2021, p. 145; OECD, *Building Organization Capacity for Public Sector Innovation*, 2014.

integrate these tools into their infrastructures, which inevitably leads them to turn to the outsourcing market[178] .

This trend places the dialectic between the public and private sectors, the administration and large companies specializing in the implementation of high-tech solutions at the center of the debate[179] . The latter are indeed called upon to contribute to the pursuit of the public interest through the provision of suitable tools to lead the digital transition of the public sector. According to some authors, there is a real relationship of subordination of the public sector to the private sector that is rooted in the inability of public administrations to formulate their digital transformation strategies and to identify the technological tools they need to implement them. To this must be added that the ICT market has been characterized by very strong concentration and is now dominated by a few multinational players. These circumstances, in fact, place public administrations and international big tech in a state of mutual interdependence. On the one hand, indeed, the big companies base an increasingly large portion of their business on institutional orders; on the other hand, we repeat, the digital transition process of public administrations would be difficult if not impossible to achieve without the contribution of private technology partners.

Well, in this path, in order to avoid a substantial heterogenesis of purposes, administrations will generally have to perform the difficult task of balancing strongly opposing interests that are equally worthy of protection. On the one hand, the pursuit of the public interest, the need to complete public infrastructure innovation projects, the increasingly efficient provision of

---

[178] D.U. GALETTA, *Transizione digitale e diritto ad una buona amministrazione*, cit., p. 109 and *therein* cited MARY C. LACITY-RUDY HIRSCHHEIM, *Information systems outsourcing; Myths, Metaphors and Reliabilities*, John Wiley & Sons Ltd, England, 1993.

[179] P. CERQUEIRA GOMES, *EU Public Procurement and innovation,*cit., p. 146;

essential public services (health, transport, telecommunications, defense, ...), according to the saying "doing more with less"; on the other hand, the legal interests of the private companies that provide the Administration with technological solutions, as well as the subjective legal positions of the end users, beneficiaries of the services provided through the aforementioned solutions, must also be taken into account.

In this paper, in particular, we will focus on the difficult balancing act, in the light of the current European regulatory context, between the right to transparency of public activity and the right to good administration in one hand and, in the other hand, the protection of trade secrets and intellectual property, of which private technology partners accompanying public administrations in the digital transition process are instead bearers.

As will be made clear, this dialectic reverberates on the public contracting system, as this is both the means by which administrations procure technological solutions and the end, as in some cases these solutions are aimed at rationalising tendering operations.

2. Public Procurement as “tool” and “purpose” of the digital transition.

In the described context, public procurement system plays a central role, constituting the paradigm for the provision of technological solutions of public administrations, thus the "tool" for the realization of the digital transition[180] , while at the same time being the "purpose" of the digital revolution of the

[180] G.M. RACCA-R.YUKINS, *The Promise and Perils of Innovation in Cross-Border Procurement,* in G.M. RACCA-R.YUKINS, *Joint Public Procurement and Innovation,* Brussels, 2019, 1; J.M. GIMENO FELIU, *Public Procurement as a strategy for the development of innovation policy*, in G.M. RACCA-R.YUKINS, *Joint Public Procurement and Innovation,* Brussels, 2019, 275.

public administration, in the sense that part of the acquired solutions can be used in the streamlining of tendering procedures[181] .

Here we will focus on the first aspect, trying to highlight the new challenges that the public procurement discipline has to face in accompanying the technological innovation process of administrations.

A large part of the technological solutions needed by public administrations to innovate their digital infrastructures are artificial intelligence (AI) systems. The European Commission, in its Proposal for a Regulation on Artificial Intelligence[182] defined an "artificial intelligence system" (AI system) as "*software developed with one or more techniques* (...)*, which can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations or decisions that influence the environments with which they interact*"[183] . If public administrations need such solutions, their procurement goes through a public tender, in application of Directive 2014/24 and the relevant disciplines of each member state.

Regardless of the type of procedure chosen, when a public administration purchases software - as combinations of computer instructions and data definitions that allow the computer hardware to perform computational or control functions[184] - it must carry out a prior technical-economic comparative assessment aimed at identifying the best solution for the case in question. In light of this, the Administration, in principle, has the possibility of: i) deciding whether to purchase *ad hoc* software based on its

[181] Emblematic in this sense is the example of some Italian authors on the "Prometea" algorithm, used in Argentina to handle public tenders for the purchase of goods and services. Thanks to the use of this system, the contract is now awarded with a 4-minute expenditure, an activity that with the "classic" procedure would have taken an average of 29 working days.

[182] COM(2021)206 final, 21 April 2021

[183] See Art. 3(1)(1);

[184] Systems and software engineering - Vocabulary (ISO/IECIEEE 24765).

specific "make option" requests; ii) reusing software or parts of software developed on behalf of the public administration; iii) purchasing *open* source code software; iv) software that can be used in cloud computing mode (where the public administration acquires the software essentially as a mere service); v) acquiring proprietary software through the use of user licenses; vi) requesting software that provides for a combination of the previous solutions.

In the Italian system, Articles 68 and 69 of the Code of Digital Administration (Legislative Decree No. 82 of 7 March 2005), after having taken up the described taxonomy, in order to favor the 'reuse' of software and avoid duplication of costs to be charged to the public purse, provides that '*public administrations that own IT solutions and programs developed on the specific instructions of the public purchaser, are obliged to make available the relevant source code, complete with documentation and released in the public domain under an open license, for* free *use*'[185] .

The provision is clearly in favor of the purchase of *open source* software, also in line with the European trend to enhance the re-use of data held by public administrations[186] .

In some cases, however, comparing the various options available on the market is very difficult and in other cases, the needs of administrations require specific operating systems that are either "proprietary"[187] or specially customized by the production company.

---

[185] See Article 69 of Legislative Decree No 82 of 7 March 2005 and AGID's '*Guidelines on the acquisition and reuse of software for public administrations*';

[186] See on this point, most recently, the Data Governance Act.

[187] As clarified in G. PASCUZZI, *Il diritto dell'era digitale,* Il Mulino, Bologna, 2020, p. 42, proprietary software is software developed for economic exploitation. The author also points out, on p. 209, that there are different ways of distributing proprietary software and among the main ones are the End User License Agreement (EULA), the General Public License and the Creative Commons Licenses.

Without pretending to deal with the technical aspects of the matter, it must be emphasized here that software is essentially represented by two codes: the “source” code, expressed in a programming language that can also be understood by humans (equipped with a certain degree of technical programming skills), and the “object” or “executable” code, which on the contrary can only be interpreted by computers. The transition from “source” to “object” is carried out by means of an additional software “interpreter”, A person who does not know the “source” code can retrieve it from the “object” code by means of a so-called “reverse engineering” mechanism, which, however, involves a considerable amount of time and money[188]. The most widespread technological tool for preventing "theft" is undoubtedly that of source code secrecy.

Consequently, as will be discussed in more detail, the protection of intellectual property with respect to software has been recognized at European level, grafted onto the logic of their commercialization in the form of the "object" code alone. The exploitation of the asset therefore takes place through contracts on the rights of economic use by means of the assignment of the asset (which entails a full and definitive transfer), or the user license (which entails a limited and temporary transfer)[189] .

Well, if the Administration decides, following purely discretionary evaluations, that it wants to acquire proprietary software, it will have to record this decision in a *lex specialis* and call for a tender to select the best contractor. Once the tender has been awarded and the technological solution appropriate to the needs of the administration has been chosen - a task of considerable complexity, with respect to which public officials often appear to lack the

[188] E. ELIAM, *Reversing: Secrets of Reverse Engineering*, Wiley, 2011.
[189] In these terms see G. PASCUZZI, *Il diritto dell’era digitale*, *cit.* p. 209;

necessary skills[190] - the software and its source code must be processed by translating factual elements and legal assumptions into an algorithm[191] . The automation of the administrative decision (or part of it) cannot indeed disregard a predetermination of the criteria for weighing the interests at stake and the specific weight of each of them. Now, for the burden of decision-making to be transferred to the machine, however, it must be given the coordinates within which to act. In essence, the administration has the task of identifying the data to be evaluated, the criteria and the objectives to be pursued (which in turn, in deference to the principle of legality must be predetermined by law). At this point, the Public Administration's indications are translated by the information technicians into codes that will go on to construct the algorithm suitable for adopting the final measure, that is, certain preliminary steps pertaining to the procedural phase.

Well, in this context, where the reference legislation and the public interest to be pursued must be translated into technical rules, it is crucial that the translation of the *technical* rule into a *legal* rule is faithful and that there is no forcing or distortion of the system.

Therefore, the role played by public authorities in the management of public tenders for the procurement of technology solutions appears crucial. This is true in the planning phase of the tender (where it is essential to choose the appropriate product for the Administration's needs and, above all, to choose whether or not to purchase proprietary software), in the management of the

---

[190] F. COSTANTINO, *Gli open data come strumento di legittimazione delle istituzioni publbiche?*, in *Pubblica amministrazione con i big data*, cit., 2019, p. 173.

[191] S. TRANQUILLI, *Il rapporto pubblico-privato nell'adozione e nel controllo della decisione amministrativa "robotica"*, in *Dir. e Soc.*, 2/2020, p. 281; D.U. GALETTA, *Intelligenza artificiale per una pubblica amministrazione 4.0?*, cit.; E. CARLONI, *I principi di legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, *Dir. Amm.,* no. 2, 2020, p. 272; N. PAOLANTONIO*, Il potere discrezionale della pubblica automazione*, cit., in *Dir. Amm*., no. 4, 2021, p. 813; S. CIVITARESE MATTEUCCI, *"umano troppo umano"*, in Dir. Pubbl., 2019, p. 16.

procedure (where it is necessary to prepare the tender documentation correctly, externalising the choices regarding the technological solutions to be purchased, as well as as awarding the contract to the highest bidder) and in the execution phase of the contract, where the public interest goals that led to the launch of the tender itself must be translated into technological solutions.

At this last stage, however, the interest of tender participants, or other private citizens, in knowing the characteristics of the actual implementation of the technological solution purchased, including the essential features of the software realized, may arise.

For the purposes of this writing, the question must be asked:

i) what can happen if the technological instruments thus constructed make errors, due to malfunctioning of the algorithm (so-called bias), or due to the erroneous translation from legal rules to machine-codes, or, under a competing profile, in the hypothesis in which the algorithm has been programmed on the basis of an illegitimate provision (perhaps due to conflict with the Constitution or European regulations) and, consequently, produces decisions *contra legem*. In such cases, the addressee of such decisions will be entitled to know the reasons for them, in accordance with the principle of good administration laid down in Article 47 of the European Charter of Fundamental Rights. Well, what is the proper depth of this knowledge? How is this latter legal position balanced with the interests -- in particular trade secrets and intellectual property rights -- of the companies that have provided, after winning a tender, the relevant technological solutions required by the public administration?

ii) whether it is wholly consistent with the principle of transparency of the activities of the public administration, irrespective of possible machine errors, that certain typically public functions are entrusted to computer systems, some of which are unintelligible and in the purely private domain.

3. Algorithmic "opacity" between the principle of transparency, the right to good administration, trade secrets and intellectual property. Perspectives *de iure condito* in the light of the European legal context.

In the context of public tenders, in general, the need for the knowability of software - manifested through the submission of a request for access to the contracting authority - may arise (i) in the course of the tender procedure, where an economic operator intends to challenge the award of another competitor; (ii) in the execution phase of a previously awarded contract, where a person with a qualified interest wishes to know how the software financed with public funds was actually developed[192] ; (iii) or again, in the event that in the execution phase of the contract, the software (due to a programming error or malfunction) makes a mistake by adopting an unlawful administrative decision.

Well, in such cases, one has to ask oneself what are the legal coordinates within which the Administration can operate the difficult balancing act between the various interests at stake, which include the interest of the

[192] On the importance of transparency in the execution phase of contracts see G.M. RACCA-R. CAVALLO PERIN-G.L. ALBANO, *Competition in the execution phase of public contracts*, in *Public contracts Law Review*, Cl. 41, no. 1, 2011, p. 99-103; Recital 122 of Directive 2014/24, moreover, specifies that "*citizens, stakeholders, whether organized or not, and other persons or bodies who do not have access to the review procedures of Directive 89/665/EEC nevertheless have a legitimate interest as contributors to the proper conduct of procurement procedures. They should therefore have the possibility, by means other than the review system provided for in Directive 89/665/EEC and without this necessarily entailing action by them before the courts and tribunals, to bring possible infringements of this Directive to the attention of the competent authority or structure.*" On the widening of the legitimacy to propose generalised civic access in the execution phase of public contracts, see Cons. St., Ad plen, April 2, 2020, no. 10.

company that supplied the software to the Administration in keeping secret its information considered to be part of its trade secrets or its intellectual property. Opposed to these latter interests are the general public interest in the transparency of administrative activity (even if exercised through software), the right to good administration enshrined in Article 41 of the Charter of Fundamental Rights of the European Union (especially where it enshrines the administration's obligation to give reasons for its decisions), and, in contentious cases, the right to an effective remedy enshrined in Article 47 of the Charter.

To shed light on the process of realization of the algorithm is not a merely "technical" matter. Indeed, as anticipated, the realization of the algorithm on which the functioning of the software deputed to the provision of public services (or to the adoption of public decisions) is based derives from the translation of the legal context of reference into machine code. The public interest objectives that the administration intends to pursue, must indeed be transformed into indications for the software deputed to their actual realization.

Understanding whether this transposition has been done correctly is one of the faculties that must be granted to any citizen in a state founded on the principle of legality and accountability of public decisions. This feature, however, encounters counterbalances that deserve to be taken into consideration by the jurist.

According to a view of the most recent Italian jurisprudence[193], favourably shared by some scholars[194], access should in general be allowed to algorithms used in the provision of public services or in the adoption of

[193] See, most recently, Cons. St., sec. VI, April 13, 2019, no. 8472.

[194] See, *ex plurimis*, N. PAOLANTONIO, *Il potere discrezionale della pubblica automazione*, *cit*., p 832; E. CARLONI, *I principi di legalità algoritmica, cit.*, p 289; A. G. OROFINO, *Intelligenza artificiale al servizio delle funzioni amministrative*, in *Giur. It*., 2020, 1738.

administrative decisions following the taxonomy of the three corollary principles of algorithmic legality, represented by the principle of transparency or "comprehensibility" of the algorithm, the principle of "algorithmic non-exclusivity" and algorithmic non-discrimination[195] . Italian jurisprudence, called upon to express an opinion on the subject following some "errors" committed by algorithms in the adoption of administrative decisions, has generally always shared the view that it would be proper to grant the citizen harmed by the decision full access to the source code for several reasons (i) the confidentiality of the companies producing the software cannot be relevant, since by providing these tools to the public administration they *de facto* accept the consequences in terms of maximum transparency; (ii) the decisions taken by means of the algorithm, even if the latter is produced by private economic operators, must be brought back into the realm of public determinations and, consequently, subject to the regime of maximum transparency.

As pointed out by some authors[196], however, such a prospect does not take due account of all the interests at stake, in particular by *a priori* frustrating the position of the economic operators that own the software and, consequently, are the owners of information that is part of trade secrets as well as of intellectual property rights. Another drawback to unconditional access to the source code is the fact that such a solution would hardly give the administrator a full account of the reasons behind the decision taken against him[197] . Among other things, there would be obvious problems of digital discrimination (the so-called *digital divide*) as it is not certain that the majority

[195] E. CARLONI, *I principi di legalità algoritmica, cit.*, p 296;

[196] F. BRAVO, *Trasparenza del codice sorgente e decisioni automartizzate*, in Dir. Inf., no. 4-5, 2020, 693; Id., *Access to source code of proprietary software used by public administrations for automated decision-making. What proportional balance of interests?*, in *European Review of Digital Administration & Law (Erdal),* 2020, 1-2, p. 157 ff;

[197] F. COSTANTINO, *Gli open data come strumento di legittimazione delle istituzioni publbiche?*, cit. 173.

of the administrators possess the appropriate tools to understand the passages of a source code. This limitation would not even be overcome by the planned translation of the code into the current language, in which there would be risky interpretations or reworkings of the code that would in fact nullify the reasons for such a choice.

For the purposes of this paper, it is necessary to dwell more specifically on the correct balance, in the light of European Union law, between the principles of transparency and good administration - which, on the one hand, would lead to the maximum openness of all information held by the public administration - and the intellectual property rights and trade secrets held by companies.

a) Principle of transparency, right to good administration and effective remedies

A first fundamental parameter for the purposes of the aforesaid balancing act is undoubtedly the principle of transparency, with respect to which in recent years European states have witnessed a veritable paradigm shift, passing from secrecy as the "rule" of the exercise of power to its exception[198]. On this point, it should be pointed out that in today's conception of “administrative transparency”, this is understood as the comprehensibility

[198] For a comprehensive reconstruction of the evolution of the principle of transparency in Italy see, without claiming to be exhaustive, A. CORRADO, *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Edizioni Scientifiche Italiane, Naples, 2018; Id, *La trasparenza nella legislazione italiana*, in *Codice dell'azione amministrativa*, edited by M.A. SANDULLI, Giuffrè Editore, Milan, 2017; Id, *Il Principio di trasparenza e i suoi strumenti di attuazione*, in *Principi e regole dell'azione amministrativa*, edited by M.A. SANDULLI, Giuffrè Francis Lefevbre, 2020, p. 124; C. COLAPIETRO-A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in *Le nuove frontiere della trasparenza nella dimensione costituzionale*, edited by C. COLAPIETRO AND L. CALIFANO, Editoriale Scientifica, Naples, 2014.

and knowability from the outside of the activity of the public administration, with particular reference to the perception of citizens[199].

A transparent Administration, indeed, through an activity that is comprehensible and knowable is able to exercise an action that takes into account the constitutionally guaranteed principles of impartiality and good performance, making citizens understand the choices made in the general interest[200]. Transparency must be considered, within the current vision of the public administration, as a fundamental and necessary value[201], an immanent value of the entire legal system, as well as a way of being of the organization of public powers aimed at finding the right connection between the requirements of guarantee and efficiency in the performance of administrative action[202].

The path that led to the aforementioned principle began in the Napoleonic Code, where the exercise of public power was conceived as secret and impenetrable to the citizen[203]. In other words, it was considered that the actions of the administration should not be knowable by the citizens, since such an approach would have meant an unnecessary aggravation of the activity carried out by the former, giving the latter a dangerous and unnecessary form of control.

---

[199] H. J. BLANKE-R PERLINGEIRO, *Essentials of the Right of Access to Public Information: An Introduction*, in H. J. BLANKE-R PERLINGEIRO, *The Right of Access to Public Information: An International Comparative International Legal Survey*, 2018, pp 2-45.

[200] A. CORRADO, *Il principio di trasparenza*, in M.A. SANDULLI (ed.), *Principi e regole dell'azione amministrativa*, Giuffrè Editore, Milan, 2017, 104; MANGANARO, *L'evoluzione del principio di trasparenza amministrativa,* in *Astridonline.it*, 2009.

[201] Thus G. ARENA, *Trasparenza amministrativa,* in S. CASSESE (ed.), *Dizionario di diritto pubblico,* VI, Milan, 2006.

[202] The Council of State expressed itself in these terms in Opinion No. 515 of February 24, 2016, rendered on the draft Decree No. 97/2016 that amended the so-called Transparency Decree (Legislative Decree No. 33/2013), which will be discussed below.

[203] On this point see C. COLAPIETRO-A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione,* cit., 117; V. FANTI, *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margin di una recente sentenza della Corte Costituzionale (n. 20/2019)*, in *Federalismi*, 5/2020.

As proof of this, in the pages of the greatest scholars of administrative law of the first half of the 20th century there is no reference to the notion of administrative transparency. An absence that seems to be due to the conception of the centralized State, whose activity was characterized by areas of unquestionable secrecy that could not be questioned, since this would have called into question an authoritarian conception of central power[204] .

One of the first jurists in Italy to draw attention to the subject was Filippo Turati who, in 1908, in a speech addressed to the Chamber of Deputies, uttered the celebrated phrase "*where a higher public interest does not impose a secret moment, the house of administration should be made of* glass."[205] . Turati's warning, however, went unheeded for several years. Indeed, it was only with the entry into force of the Italian Constitution, which in Article 97, paragraph 2, states that public offices are organized according to the provisions of the law, in such a way as to ensure the good performance and impartiality of the administration.

The introduction of the principles of impartiality and good performance in the Constitutional Charter also gives a solid foundation to the corollaries of publicity and transparency of administrative action. This is because, by guaranteeing that the Administration's actions are known to the people administered, it also allows for a form of widespread control over compliance with the aforementioned constitutional principles of impartiality and good performance[206] . Transparency, at the same time, with the entry into force of the Constitution, has become an aspiration of the Administration imposed by

---

[204] In these terms see V. FANTI, *Administrative transparency between constitutional principles and values of the European order: in the margin of a recent Constitutional Court ruling (no. 20/2019)*, cit. p. 36.

[205] F. TURATI, *Discorsi parlamentari,* Camera dei Deputati, Sessions 1904-1908, June 17, 1908, 22962.

[206] Significant on this point is the passage of the Constitutional Court judgment, February 27, 2019, no. 9, where it is Stated that "*the principles of publicity and transparency, referring not only, as a corollary of the democratic principle (art. 1 Const.), to all relevant aspects of public and institutional life, but also, pursuant to art. 97 Const., to the proper functioning of the administration.*"

the democratic principle under which the legitimacy of rulers is strongly represented by the knowability of their actions by the electing citizens. In this way, the relationship between public power and citizens gradually changed, no longer conditioned by the authority-freedom binomial but rather by the function-interest binomial[207] .

Well, this fundamental principle also inevitably impinges on those public interest activities exercised by means of algorithms, which is why, according to some authoritative scholars, in such cases "*liberty and democracy will depend to a significant degree on the extent to which these algorithms and their functioning can be made transparent to the* public"[208].

As has been observed by some scholars[209] , moreover, with respect to the new technologies, transparency can take on two different meanings, such as "*fishbowl transparency*" (which basically concerns the right of citizens to be fully aware of and acquire information on the work of the public administration, along the lines of the Freedom of Information Act of Anglo-Saxon origin) and "*reasoned transparency*" (more focused on explaining the reasons underlying administrative decisions). These parameters must, in the writer's opinion, both be taken into account and applied to the concrete case in light of the principle of proportionality.

Well, in the case of automated decisions, i.e. provided through the use of software based on algorithms, a model of transparency by *design* or *by*

---

[207] Thus C. COLAPIETRO-A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, cit., 118; on this point, some overseas authors have pointed out that '*Transparency is integral to legitimate governement and fai society. When government is open, officials can be expected to do their jobs better because public accountability presumably inhibits them from advancing their own self-interests at the expense of their duty to produce public value*'. In these terms see C. COGLIANESE-D. LEHR, *Transparency and algorithmic governance*, in *Administrative Law Review*, 71:1, 2019, 18.

[208] C. COGLIANESE-D. LEHR, *Transparency and algorithmic governance*, in *Administrative Law Review*, 71:1, 2019, 3.

[209] C. COGLIANESE-D. LEHR, *Transparency and algorithmic governance*, cit. p. 19.

default[210] should theoretically be guaranteed, in the sense that the intelligibility of the logic underlying the system should be guaranteed *ex ante*, at the time of programming. According to some scholars, in other words, transparency would constitute 'the *quintessential solution*' to the opacity of algorithms[211]. As noted by other scholars of the subject, however, it is not obvious that the openness of the algorithm inevitably entails its accountability[212].

The principle of transparency is also immanent in the field of public contracts[213] (consider that in Directive 2014/24 the term "transparency" appears no less than 24 times), where it performs the task of safeguarding and coordinating the balancing of various interests at stake, such as competition, *equal participation*, control over the proper investment of public resources and the regular conduct of tenders and respect for the principle of legality, as well as the fight against corruption[214]. The principle is of central importance from the drafting of the tender documents to the conclusion of the contract, as well as in the execution phase. According to some authors, "*public contracts should be treated as public information, and should in principle be accessible accordingly. (...) this default disclosure should prevail over private interests*

---

[210] D.U. GALETTA, *Algoritmi*, *procedimento amministrativo* e *garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in RIDPC, no. 3, 2020.

[211] M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, in *AIDA*, 2018, 199; SCHWARTZ, *Data processing and Government Administration: The Failure of the American Legal Response to the Computer*, in Hastings L.J., 1992.

[212] M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, cit. p. 204; DESAI-KROLL, *Trust but verify: a guide to algorithms and the law*, in *Harvard Journal of Law & Technoloy*, 2017, 1.

[213] S. ARROWSMITH, *The Purpose of the EU Public Procurement Directives: Ends, Means, and the Implications for National Regulatory Space for Commercial and Horizontal Policies*, 2012, 14 Cambridge Yearbook of European Legal Studies 20-25, where the Author points out four dimensions of transparency in public procurement law: i) publicity for contract opportunities; ii) publicity of the rules governing each procedure; iii) a principle of rule-based decision-making that limits the discretion of contracting authorities or officers; and iv) verification and enforcement of the rules.

[214] In this respect, the CJEU, in its judgment of 7 December 2000, C-324/98 *Telaustria,* clarified in paragraph 62 that the obligation of transparency "*consists in ensuring, for the benefit of any potential tenderer, a degree of advertising sufficient to enable the services market to be opened up to competition and the impartiality of procurement procedures to be reviewed.*"

in confidentiality of contract clauses"[215]. On this point, it has also been argued that "*a default requirement of disclosure*" with respect to information on public contracts can be derived from the general principles of European procurement law[216] .

A direct corollary of the principle of transparency is the right to good administration enshrined in Article 41 of the European Charter of Fundamental Rights[217] , which includes in particular (i) the right of every individual to be heard before an individual measure adversely affecting him or her is taken; (ii) the right of access to the file concerning him or her; and (iii) the obligation for administrations to give reasons for their decisions. This principle, moreover, has been given the status of a general principle of Union law by the Court of Justice[218].

These parameters are closely related - allowing their full expression - to another fundamental right enshrined in Article 47 of the European Charter of Fundamental Rights of the European Union, namely the right to an effective remedy[219] . The right to be able to activate a procedural instrument before a judge against an administrative decision considered unlawful is indeed intimately connected with the full knowledge of the reasons underlying that decision. Well, the potential contrast between this assumption and the ontological opacity of automated decisions is evident, especially if the

---

[215] C.GINTER-N.PARREST-M.A.SIMOVART, *Access to the content of public procurement contracts: the case for a general EU-law duty of disclosure*, in *Public Procurement Law Review*, 2013, 4; E. PLAS, *Amendements tu public contracts: in searcg of a sufficient degree of transparency*, in *Public Procurement Law Review*, 2021, 1;

[216] M.A. SIMOVART, *Old remedies for new violations? The deficit of remedies for enforcing public contract modification rules*, in *UrT*, 2015/1, pp 33-47.

[217]D.U. GALETTA, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione,* in Riv. It. Dir. Pubbl. Com., no. 3, 2005, p. 819.

[218] See, *ex plurimis*, CJEU, 10th of February 2022, C-219/20, LM.

[219] On the link between the right to good administration and the right to an effective remedy see, *ex plurimis,* CJEU, October 10, 2012, C-183-10, *Global Development*, para. 40; Id., April 27, 2017, C-556/11 *European Dyinamics*, para. 153.

technological tools that underpin them are the subject of intellectual property or trade secrets.

In the light of the above, it is therefore necessary to try to understand what tools the jurist in the European context possesses to adopt the correct balance of the interests at stake, in order to avoid an excessive compression of the positions of the technological partners of the public administration, as well as an excessive burdening of the administrative burden linked to the total transparency of the administration's work.

b) Intellectual property, trade secrets and software protection

If, on the one hand, as we have seen, Article 41 of the Charter of Fundamental Rights of the European Union, by providing the right to good administration, requires the public decision-maker to indicate the reasoning behind his decisions, on the other hand, Article 17(2) of the same Charter elevates the right to intellectual property to the status of a fundamental right, stating that the latter "*shall be protected.*" This inevitably places the two fundamental rights - the right to a statement of reasons for public decisions and the right to the protection of intellectual property - on the same level, without providing any particular elements to guide the balancing act between them, which must therefore be found by a systematic reading of the special legislation.

In this regard, it must be premised that the protection of intellectual property, especially in the area of public contracts, must be read in the light of the principle of fair competition between economic operators, in the sense that the latter value could be called into question if confidential commercial information is publicized without due consideration.

Turning to an examination of the special legislation on the subject, it should first be noted that the Directive on the Protection of Confidential Know-How and Confidential Business Information (2016/943/EU) defines in Article 2(1)(1) as falling within the scope of the legislation information that: (i) is secret; (ii) has a commercial value as a secret; and (iii) has been subject to reasonable measures to maintain it secret. The definition, which is indeed quite broad, is certainly capable of covering software and algorithms that meet the above-mentioned requirements[220] . It is necessary here to highlight the hypotheses in which the legislation allows trade secrets to be compressed as such for the protection of overriding interests. In this regard, Article 1(2)(b) expressly provides that the Directive is without prejudice to the application of Union or national rules requiring the holder of the trade secret "*to disclose, for reasons of public interest, information including trade secrets, to the public or to administrative or judicial authorities for the performance of their duties of those authorities".* Under a concurrent profile, the subsequent Article 11 provides that judicial authorities, when judging on the application of the measures for the protection of secrets (and therefore when deciding whether or not to disclose information) shall take into consideration specific circumstances including the public interest (point g) and the protection of fundamental rights (point h). In other words, the directive would seem to require the judicial authorities called upon to rule on the disclosure of secret information to strike an appropriate balance between the interest in secrecy and the public interest and the protection of fundamental rights. This intention is also made explicit in Recital 20 - where it is significantly stated that "*the protection of trade secrets (...) should not extend to cases where the disclosure of a trade secret serves the public interest*" - and in Recital 11, according to

[220] M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, cit. p. 205.

which the Directive should not affect the application of Union and national rules providing for the disclosure of information, including trade secrets (this refers in particular to rules on public access to documents and transparency obligations on the part of national public authorities).

The outlined System of the Trade Secrets Directive is characterized by a marked sensitivity to the protection of such information, which in principle can only be withdrawn in the presence of *disclosure* requirements linked to the pursuit of public interests or with respect to the protection of fundamental rights of citizens. The protection of trade secrets, according to the European framework would in other words be subordinate to the protection of overriding interests, where there are national or European rules that impose the necessary disclosure of information[221] .

In turn, in the directive on the legal protection of software (2009/24/EU, implemented in Italy by amending the Copyright Law), as noted by some authors[222] , the balance between protecting intellectual property and protecting the market is carried out without compromising the secrecy of the source code and intellectual property rights. In particular, the aforesaid balancing act is carried out by means of the institute of decompilation, which consists in the faculty for the party wishing to make its own software interoperable with another 'proprietary' software, to proceed without authorization to obtain the necessary information, without providing for the disclosure of the source code.

Another regulatory framework that is useful from a hermeneutic point of view to address the subject matter of this paper is undoubtedly the GDPR, which enshrines, in the case of automated processing of personal data, the right

[221] M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, cit. p. 213.
[222] F. BRAVO, *Trasparenza del codice sorgente e ddecisioni automatizzate*, cit. p. 705.

of data subjects to obtain from the data controller "*meaningful information about the logic involved*" (Art. 15(1)(h)). In this regard, the legislator itself, in recital 63 of the GDPR, after reiterating that every data subject should have the right to know the logic involved in any automated data processing, specifies that "*that right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular copyrights protecting the software*". In other words, the European legislator, even in this case, imposes a balancing act between the data subject's right of access (and to transparency) and the interest in the secrecy of the business information of the entities that provided the technological solution through which the personal data were processed, while not obliging the disclosure of confidential business information[223] .

In essence, the *ratio of* the aforementioned decisions would appear to be that of rendering effective and efficient the release of information so that it acquires value for the purpose of explaining the logic of the processing used, by making the data subject aware not of the technical instructions given in programming language for the operation of the software deputed to the adoption of the automated decision, but of intelligible information that can enable him to learn the operating methods, criteria and parameters used to reach the decision[224] . This approach, which seems to be inspired by the paradigm of "reasoned transparency" mentioned above, constitutes a reasonable compromise, albeit one that is difficult to apply and centred on *ex*

[223] The *Data Governance Act* also seems to have shared this approach, where it has placed express limitations on the re-use of data held by public administrations, where these are considered as trade secrets, i.e. the subject of intellectual property (see in particular Article 3 and Recitals 10, 18 and 20).

[224] F. BRAVO, *Source code transparency and automated decisions*, cit. p. 712;

post knowability of the reasons underlying automated decisions and not instead, as would be more desirable, *ex ante*[225] .

Well, these principles must be read in the light of the European public procurement rules, with particular reference to Directive 2014/24, which expressly states in Article 21 that "*Unless otherwise provided in this Directive or in the national law to which the contracting authority is subject, in particular legislation concerning access to information, (...)the contracting authority shall not disclose information communicated by economic operators which they have designated as confidential, including but not limited to, technical or trade secrets and the confidential aspects of tenders*".

The Court of Justice ruled on the correct interpretation of the provision in its judgment of September 7, 2021 in Case C-927/19, which deserves to be mentioned for having attempted to provide a systematic reading of the reference framework, in order to identify the correct balance between Article 21 of Directive 2014/24 on trade secrets and the right to the disclosure of such information for defensive purposes (in comparison with the "remedies" Directive 89/665, which became Directive 2007/66). On this point, the Court first stated that Article 21 of Directive 2014/24 provides that the contracting authority shall in principle not disclose information communicated by economic operators and considered confidential also under Directive 2016/943. In this regard, the Court recalled that the main objective of the EU public procurement rules includes the opening up to undistorted competition in all member states and that, in order to achieve this objective, it is necessary

[225] In a critical sense S. WACHTER-B. MITTELSTADT-L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, (December 28, 2016), in *International Data Privacy Law*, 2017, Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469; R. MESSINETTI, *The Protection of the Human Person versus Artificial Intelligence. Decision-making power of the technological apparatus and the right to an explanation of automated decision-making*, in *Contract and Enterprise*, no. 3, 2019, 870.

that contracting authorities do not disclose information relating to tender procedures, the content of which could be used to distort competition, either in the current procedure or in subsequent procedures.

In this case, the public administration, faced with a request for access by a competitor who was not awarded the tender, had refused it because the information whose publication was requested was considered to be a trade secret (of which the successful tenderer was the owner)[226] . On this point, the Court, echoing the conclusions presented by the Advocate General, specified that an administration that denies access to information because it is considered a trade secret must also explain the reasons why that information is not admissible. On this point, the Court recalled that in accordance with the right to good administration laid down in Article 41 of the Charter of Fundamental Rights of the European Union (see *above),* public authorities are under an obligation to give reasons for their decisions, also in order to allow the addressees of those decisions to defend their rights and to decide in full knowledge of the facts whether a judicial remedy should be brought against them. From a concurrent point of view, the duty to state reasons is also necessary to enable the courts to review the lawfulness of those decisions, thus constituting one of the conditions for the full exercise of effective judicial remedies under Article 47 of the same Charter[227].

It follows that if the Administration intends to reject an application for the disclosure of an economic operator's business secrets (in the course or at the outcome of a tender procedure), it must adequately explain in its reasoning

[226] However, it is believed that the principles expressed by the Court can also be extended to the hypotheses of private citizens who did not take part in the tender but wish to know the award criteria, the reasons that led the administration to judge the winning bid as the best one and the characteristics of the technological solution selected, if any, that will be used for administrative decision-making.

[227] EUCJ, 9th November 2017, LS Customs Services, C-46/16, EU:C:2017:839.

the balance struck between the undertaking's interest in the confidentiality of the information and the interest of the applicant in the specific case. Only a precise statement of reasons in respect of that balancing will allow the applicant's right of defense to be fully exercised and, consequently, in the event of an appeal before the court, the exercise of a full and effective review in compliance with the standards laid down by Article 47, itself set out in Directive 2007/66[228].

Significantly, the decision essentially provides that the Administration, in order to carry out the aforementioned balancing of the various interests at stake, must know the information qualified as "confidential" by the economic operator. The same information, again for the purpose of a correct balancing of the conflicting interests, must also be known by the judge in court, who may, if he deems it necessary, not withhold that information from the other parties[229].

The decision, while having the merit of having made some progress on the issue at hand, has nevertheless been criticized by some scholars for having essentially avoided taking a clear position (despite having the opportunity to do so) on the actual modalities - as well as the benchmarks - by which the Administration (initially) and the judge (in the event of any litigation) should decide whether to value the secrecy of business information or the conflicting interests related to the disclosure of such information.

4. Perspectives *de jure condendo in the* light of the proposed regulation on AI

[228] On the "multifunctional" nature of the motivation of an administrative measure, thus aiming at the comprehensibility of the administration's actions (transparency requirements) as well as the full exercise of the right of defense of the addressee of the decision (defense requirements) see F. CARDARELLI, *La motivazione del provvedimento,* in *Codice dell'Azione Amministrativa*, edited by M.A. SANDULLI, Milan, 2016, 397.

[229] See points 130 and 131.

The European Unio''s sensitivity to these issues is also evident from the first signs to be found in the Proposal for a Regulation on Artificial Intelligence[230] approved by the Commission on 21 April 2021, and in respect of which Parliament published an initial Draf Report with additions on 20 April 2022 . Without being able to examine the Proposal in its entirety, we will limit ourselves to noting that with this act, the European legislator intended, on the one hand, to fill the concept of algorithmic transparency with specific contents, enucleating a series of obligations for Administrations as well as for economic operators aimed at making the logic behind the functioning of algorithms more intelligible; on the other hand, it attempted to further highlight the need for protection that the system must reserve for certain commercial information that is considered "secret".

In particular, as early as point 3 of the preamble (p. 12), the Regulation specifies that "*the increased transparency requirements will not disproportionately affect the right to protection of intellectual property (Article 17(2)), as they will be limited only to the minimum information necessary for persons to exercise their right to effective recourse and necessary transparency with control and law enforcement authorities, in line with their mandates. Any disclosure of information will be made in accordance with relevant legislation in the field, including Directive (EU) 2016/943 on the protection of confidential know-how and confidential business information (trade secrets) against unlawful acquisition, use and disclosure. Public authorities and notified bodies, when they need access to confidential information or source code to examine compliance with substantive obligations, are subject to binding confidentiality obligations*".

[230] COM (2021)206.

Recital 47, in turn, provides for that "*to address the opacity that can make certain AI systems incomprehensible to natural persons, a certain degree of transparency should be required on high-risk AI systems. Users should be able to interpret the system outputs and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use, and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate*". In the same sense, Article 13 does not seem to advocate indiscriminate transparency, providing on the contrary that "*high-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and level of transparency shall be ensured* (...)".

A novelty of great interest is that provided for in Article 60, which consists in the creation of a database at European level where all 'high-risk' artificial intelligence systems are to be registered, with the information contained in Annex VIII of the Regulation (trade name, purpose of the system, instructions for use and certificates of conformity), in order to make it accessible to anyone with an interest[231].

As mentioned above, the Commission's proposal has already passed the initial scrutiny of Parliament, which in the first draft published on April 20,

[231] This solution, however, seems to have been preconceived in the English system: House of Commons, Algorithms in Decision-Making: Fourth Report of Session 2017-19 , HC 351, May 23, 2018, paras 3-45. In this report, it was advocated that the British government should play its part in the algorithms revolution in two ways. First, it should continue to make public sector datasets available for 'big data' developers, but also for algorithm developers. Second, the government should produce, publish and maintain a list of where algorithms with impact are being used by the central government, along with projects underway or planned for public sector algorithms, to aid not just private sector involvement, but also transparency, which is a public value (para 30).

2022[232] made a number of changes, among which, as far as we are concerned, we note the insertion of Recital 80 d), which describes a series of inspection powers of the Commission with respect to the implementers of AI systems, among which emerges the power to request companies or public authorities to access "databases, algorithms and source codes". Also significant is the specification in the final explanatory statement, where it is made clear that if the user of artificial intelligence systems is a public authority, this will be "*subject to increased transparency exposures in democratic societies. As such, public authorities (...) should register the use of high-risk AI systems in the EU-wide database. This allows for increased democratic oversight, public scrutinity, and accountability, alongside more transparency towards the public on the use of AI systems in sensitive areas impacting upon people's lives*".

The approach of the European legislator would seem to be that of wanting to centralise control over artificial intelligence systems, imposing a high degree of transparency - especially with reference to high-risk systems - while maintaining the commercial interests of the companies producing these systems. It would seem to be an approach that is far from being completely 'open', but on the contrary inspired by what some American scholars have defined as 'reasoned transparency', parameterised on respect for the principle of proportionality: not ostensibility at all costs, but transparency that allows an acceptable degree of intelligibility of algorithmic decisions.

5. First concluding remarks

The public sector entrusts the performance of an increasing portion of its functions to technology. The pervasiveness in people's lives of decisions taken by means of technological tools increases and, consequently, so does the

[232] 2021/0106(COD).

risk of fundamental rights being sacrified. On the other hand, as has been pointed out, in the current context of digital transition, the public sector needs the support of private economic operators who will only continue to invest if they are guaranteed a secure legal framework that protects them from excessive compression of their intellectual property rights[233].

Specifically, the balance between, on the one hand, the interest of undertakings in maintaining the secrecy of the functioning of the technological solutions used for the adoption of public decisions (an expression of the broader right to intellectual property sanctioned by Article 17(2) of the Charter of Fundamental Rights of the European Union) and, on the other hand, the interest in full *disclosure* of such information in order to ensure the full exercise of the rights to good administration (Article 41) and to an effective remedy (Article 47), must be carried out with extreme rigour by the Administrations. Indeed, the latter, as recently confirmed by the Court of Justice, must be aware of the reasons for the secrecy of the information and consequently grant or deny access, stating the reasons for the decision with a stronger statement of reasons. Moreover, in principle, Article 52(1) of the Charter emphasizes that "*Any limitations on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only where they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others*". Consequently, a compression of a fundamental right enshrined in the Charter is permissible, but

[233] On the importance of a certain regulatory framework for private investment in the public sector to be stimulated see M.A. SANDULLI, *Principi e regole dell'azione amministrativa. Riflessioni sul rapport tra legge e realtà giurisprudenziale*, in *Federalismi*, no. 23/2017; Id., *Conclusioni ad un dibattito sul principio alla certezza del diritto*, in *Principio di ragionevolezza delle decisioni giurisdizionali e diritto alla sicurezza giuridica*, edited by F. FRANCARIO and M.A. SANDULLI, Naples, 2018, 305.

it must: i) be provided for by law; ii) respect the essential content of the right compressed; iii) comply with the principle of proportionality and iv) pursue objectives of general interest recognized by the Union.

In any case, despite the fact that, as we have seen, the current legal framework attempts to provide some guidance to public administrations (and judges) in order to correctly balance the conflicting interests at stake, the margins of discretion still appear too wide, with the obvious risk of compressing one or the other position worthy of protection in the absence of the necessary legal certainty. This context of substantial uncertainty inevitably reverberates on the ongoing digital transition process, risking inhibiting large technology companies from investing in the public sector because it is too risky for their business. At the same time, an excessively strict drift in the protection of companies' trade secrets would risk unacceptably frustrating the positions of citizens, or of competing companies, with serious prejudice to the principles of transparency of administrative activity and accountability of public decisions taken by means of technological tools.

Well, in deference to the rule of law, it is to be hoped that the European legislator, by further intervening on the acts currently being adopted, will be able to strengthen the reference regulatory system (the first signs, as we have seen, have come from the AI Act). A fundamental role, however, will have to be played by the Court of Justice of the European Union, which until now has perhaps been too timid on the subject, and which will be able to provide further hermeneutic indications on the correct composition of the various interests at stake, in light of the regulatory provisions contained in the directives.

CHAPTER 4

Concluding remarks. The impact of technological innovation in the dialectic between public and private actors: is there an evolution of the traditional dichotomy?

In light of the analysis conducted let some initial insights be allowed.

In the outlined context of rapid evolution, where the actors and interests at stake are changing, it seems crucial to think about the possible reorganization of the reference discipline as well as a greater enhancement of cooperation between public and private actors.

As we have seen, the relationship between public and private actors is as peculiar as ever in the field covered by the present analysis: the state invests in innovation in order to stimulate the development of new technological solutions, arriving at being considered as itself as an "innovator" subject[234] ; the state in turn is the first user of the aforementioned solutions, which inevitably accompany the public administration in the process of digital transition (as seen, innovation that impacts both the organization and the activity of the public administration); in turn, both public and private entities involved in the digital innovation of public infrastructure actively participate in the implementation of the process of the digital transition of the Public Administration (also with reference to the implementation of the cyber defense strategy).

In such a scenario, the regulations on the awarding of public contracts (*i.e.,* of the rules of the game) must be clear and ensure *ex ante* knowability of market access conditions.

[234] M. Mazzuccato, *Lo Stato innovatore*, Bari, 2014.

Economic operators, in other words, must be fully capable of identifying the constraints and technical standards they are required to meet, as well as the liabilities they face by approaching the public contracting market in the provision of technology solutions for public administration.

Only with sufficient certainty (or calculability, predictability) of the law, indeed, can the proper fulfillment of the ongoing digital transition process be ensured, allowing private companies to approach the public contract market having full knowledge of: i) the requirements needed to participate in tenders, ii) the "whether" and "how" elements pertaining to the cybersecurity profile will be considered when evaluating the offer, and iii) what degree of "knowability" and transparency the provided technologies will have to meet.

After all, as noted by authoritative scholars, a condition of legal uncertainty can only negatively impact the growth of a state, the performance of the market[235] as well as, in this case, the phenomenon of digital transition of government.

With specific reference to the issue of cybersecurity, it is agreed with those who believe that the phenomenon of security of public digital

---

[235] On the topic, among all, see M.A. SANDULLI, *Il ruolo dei principi nel diritto amministrativo. Introduzione a Principi e Regole dell'azione amministrativa – Quarta Edizione 2023*, in www.giustiziainsieme.it where the author lucidly elucidates that "*In a constitutional State of law, the power to authoritatively interfere in the legal sphere of others must be evidently defined and delimited by a clear and certain normative context (principle of legal certainty, declined in the principle of legality), i.e., by prior legal rules, general and abstract, more or less stringent (to which corresponds the graduation of administrative power from binding to discretionary (on which see the appropriate contribution immediately below), of a substantive (fixing of objectives to respond to specific public interest finalities) and procedural (competence, mode and timing of action, effects, etc.), which ensure the impartiality of public action ...) and the best balance of the various interests (public and private) involved (principle of good administration ...).Compliance with these rules must, moreover, be ensured through appropriate systems of control (internal and external) and, above all, through adequate modes of judicial protection (principle of effectiveness of protection), which, tendentially, justify a special system of administrative justice (which may or may not provide for the establishment of a judicial apparatus different and autonomous from the ordinary one).*" On this topic, see also F. ZACCARIA, *La perdita della certezza del diritto: riflessi sugli equilibri dell'economia e della finanza pubblica*, Pavia, 2003; C. MIRABELLI, *Il rischio da diritto. Il costo dell'incertezza ed alcune possibili economie*, in *La certezza del diritto - Un valore da ritrovare - Atti del convegno*, Firenze, 2-3 ottobre 1992, Milano, 1994, 39.

infrastructures should be inspired by a "collaborative-oriented" relationship between public and private entities,[236] into which must be grafted a profound process of training and awareness-raising of public officials on the subject, as well as an involvement of private parties in the refinement of regulation (perhaps through a dialogue on the model of *notice and comment* with the National Cybersecurity Authority). This would make it possible to alleviate the critical issues arising from information asymmetry and the phenomenon of so-called *lock-in*, freeing public administrations from the state of constant subordination vis-à-vis large companies supplying technological solutions, and, for the effect, allowing the same contracting stations to strategically orient their purchasing needs and to more knowledgeably predefine both access requirements and award criteria. Collaboration, in other words, must be carried out from the technology design phase to its use by the Administrations in the exercise of public power, passing through the regulation phase.

In this context, the role of the "Digital State[237] is thus evolving.

Administrative activity as a whole is being transformed, both in terms of modes and tools, through the application of new technologies. Whether it is a matter of security or public services, the construction of infrastructure or the exercise of justice, currency or defense, health or spatial planning, there is a

---

[236] S. ROSSA, *Cybersecurity e pubblica amministrazione,* cit., 221. In the same vein, the document bearing the "National Cybersecurity Strategy," published by the Italian Council Presidency in May 2022, States that transversal to the objectives of the strategy is the public-private partnership, marked by "*a whole-of-society approach, which sees the public sector acting synergistically with the private sector, academia and research, the media, families and individuals to strengthen the cyber resilience of the nation and society as a whole. The cyber space, moreover, consists of ICT products and services made or delivered mainly by private entities. For this reason, the present strategy cannot disregard full collaboration and constant public-private consultation, (...).*" On this point also L. PREVITI, *La collaborazione pubblico-privato nel sistema multilivello di sicurezza cibernetica*, in *La sicurezza nel cyberspazio*, edited by R. URSI, Franco Angeli, Milan, 2023, p. 157, where the author examines the current national legal context highlighting all its limitations with respect to an effective collaborative dynamic between public and private subjects.

[237] L. TORCHIA, *Lo Stato digitale¸cit.* 19; B. CAROTTI, *Sicurezza cibernetica e lo Stato-nazione*, in *Giorn. Dir. Amm*., 5, p. 629.

need for the use of technological tools that impose a reorganization of the functions of public structures, as well as the redefinition of the rules for the exercise of public power and the related modes of control. This is also with reference to liability profiles where, as observed by some authors, the ability of private power to escape a strict regime of accountability - a regime that is an integral part of a public power of a democratic nature - gradually diminishes along with the growth of private power, which comes to take on the guise of public power, an essential infrastructure or a public utility network[238].

In competing aspects, technological development impacts economic and social relations to such an extent that existing rules are often inadequate. Hence the need for new public regulation aimed at updating existing disciplines as well as introducing new principles and rules for new phenomena, as is the case with cybersecurity and the use of artificial intelligence in the public sphere.

Public subjects must therefore relate to new "powers"[239] that are posing as legal orders, endowed with regulatory power, executive power and jurisdictional power, with a scope of reference-global-much broader than the territory that generally constitutes the limit of a nation-state.

Large multinational corporations wield effective power that is able to impose, on both public and private entities, their own rules and economic conditions. On the theoretical level, the power of such corporations constitutes an antagonistic element to the democratic state in terms of public control of economic activities. In multinational corporations, in essence, power is recognized as a constitutive and ontologically given element, once belonging to states through the social contract, now subtracted from them and

[238] L. TORCHIA, *Lo Stato digitale ¸cit.* 28.

[239] M.R. FERRARESE, *Poteri nuovi,* Bologna, Il Mulino, 2023; L. CASINI, *Lo Stato nell'era di Google*, in *Riv. Trim. Dir. Pubbl.*, 2019, 1125; Id., *Lo Stato nell'era di Google*, Milan, 2020; Id., *Lo Stato (Im)mortale. I pubblici poteri tra globalizzazione ed era digitale,* Milan, 2022.

reincarnated in capitalist accumulation, which regenerates it by manifesting itself always the same, but deprived of the democratic control that constituted its necessary limit[240].

Thus, there is also a problem of containing and regulating the powers of these entities, to which some states have responded with legislation of a general nature. At the European and national levels, as we have seen, an organic legal framework has not yet been arrived at, and public administrations, which are increasingly resorting to technological solutions for the exercise of their activities, in turn require an updating of the principles and rules that have traditionally inspired their action. The principles of legality, impartiality, transparency, procedural safeguards, discretion, and all the principles and categories of administrative law in the context of the digital transition are undergoing a "shake-up" that in some cases requires them to be rethought or updated.

The public and private spheres are in the position of having to co-manage the digital transition process, albeit from different angles. Therefore, it makes no sense to think of legal experience within the opposition between public and private, and it is rather necessary to replace it with a new paradigm, characterized by "*interchangeability of roles, modification of relationships, and trade in rules and* ordering *principles*"[241]. Indeed, although "public" and "private" appear to be antithetical categories, frequently enclosed in the antipodes state-market, authority-freedom, special-interest-general interest,

[240] A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020, 56.

[241] S. CASSESE, *L'Arena pubblica. Nuovi paradigmi per lo Stato*, in *Riv. trim. dir. pubbl.,* 3, 2001, p. 601.

power-consent, the “boundaries” between the two categories seem to be more blurred today[242].

Public-private collaboration can be explicated both on the theoretical level, in relation to the collaborative leadership relationship with private entities, and on the practical level, through the development of certain projects aimed at achieving public autonomy of micro-component production, or aimed at the construction of state digital infrastructure[243], with the express purpose of overcoming one of the main obstacles to the digital transition: the oligopoly of large technology companies, which have a peculiar position in that they pursue private interests but are at the same time owners and producers of technological solutions aimed at pursuing the public interest.

The current framework, in essence, calls for a reprioritization, and a more forward-looking role for the state is required, capable of outlining national strategies aimed at directing private partners in managing the transition, strengthening public evidence rules for technology procurement, with the aim of strengthening organizational resilience in different areas, all with increasingly close cooperation between the public and private sectors.

---

[242] A. ZOPPINI, *Il diritto privato e i suoi confini*, cit., 239, where the author argues that the most convincing answer is to be found in Salvatore Pugliatti's Statement in *Voce Diritto Pubblico e diritto* privato, in *Enciclopedia del* diritto, Milan, 1964, XIII, p. 696, that "*every crisis in the field of law leads the scholar back to the distinction between public and private law.*"

[243] Such as the case of the National Strategic Pole discussed in Chapter II, which was implemented under the public-private partnership podium.

BIBLIOGRAPHY

T. AHMED, *GovTech: An Emerging Sector Revolutionising Public Services*, in www.govtechresearch.com.

G.A. AKERLOF, *Market Signaling. Informational transfer in hiring and related screening processes*, Harvard University Press, Cambridge, 1974.

I. ALBERTI, *Parteciapzione procedimentale per legittimare gli algoritmi nel procedimento amministrativo*, in R. CAVALLO PERIN (ed.), *Pubblica amministrazione con I big data*, *cit.*, pp. 285 ff..

G. ARENA, *Agenzia amministrativa,* in *Enc. Giur. Treccani*, Roma, 1999.

G. ARENA, *Trasparenza amministrativa,* in S. CASSESE (ed.), *Dizionario di diritto pubblico,* VI, Milan, 2006.

S. ARROWSMITH, *The Purpose of the EU Public Procurement Directives: Ends, Means, and the Implications for National Regulatory Space for Commercial and Horizontal Policies*, 2012, 14 *Cambridge Yearbook of European Legal Studies*, 20.

G. AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Naples, 2019;

J. AZRILYANT, *The Cyber Privatization Problem: Navigating the Law of Armed Conflict Implications of Outsourcing offensive Cyber Operations*, in *Public Contrac Law Journal*, 50, 4, 2021, 597-622.

F. BENVENUTI, *Funzione amministrativa, procedimento, processo,* in *Riv. Trim. dir. Pubbl*., 1952, I, 118.

R. BIFULCO, *Art. 41. Right to good administration*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (eds.), *L'Europa dei diritti. Commentario alla Carta dei Diritti Fondamentali dell'Unione Europea*, Bologna, 2001, pp. 290.

H. J. BLANKE-R PERLINGEIRO, *Essentials of the Right of Access to Public Information: An Introduction*, in H. J. BLANKE-R PERLINGEIRO, *The Right of Access to Public Information: An International Comparative International Legal Survey*, 2018, pp 2-45.

D. BOLOGNINO-A.CORRADO-A.STORTO, *Digitalizzazione e pubblica amministrazione*, in *Il diritto dell'era digitale*, edited by R.GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO, Milan, 2022, p. 625.

S. BONETTI, *La partecipazione strumentale*, Bologna, 2022.

B. BOSCHETTI, *La transizione digitale della pubblica amministrazione verso il modello Governement as a platform*, in A. LALLI, *Pubblica Amministrazione nell'era digitale*, Giappichelli, Turin, 2022.

F. BRAVO, *Trasparenza del codice sorgente e decisioni automatizzate*, in Dir. Inf. and Inf., 2020, I, 694.

F. BRAVO, *Access to source code of proprietary software used by public administrations for automated decision-making. What proportional balance of interests?*, in *European Review of Digital Administration & Law (Erdal),* 2020, 1-2, p. 157 ff;

R. BRIGHI-P.G.CHIARA, *Cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in Federalismi, no. 21/2021.

B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato*, in Federalismi, no. 14/2020.

E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica*, Turin, Giappichelli, 2023.

A.M. CALAMIA - V. VIGIAK, *Diritto dell'Unione Europea,* Giuffrè, Milano, 2018.

V. CAMPANILE, *Art. 19*, Public Contracts Code edited by C. CONTESSA - P. DEL VECCHIO, Naples, 2023.

R. CARANTA-FERRARIS, *La partecipazione al procedimento amministrativo,* Milan, 2010, 37

L. CARBONE, *La scommesa del codice dei contratti pubblici e il suo futuro*, in giustizia-amminsitrativa.it, 2023.

F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. Inf.*, 2/2015, 227 ff.

F. CARDARELLI, *L'uso della telematica*, in *Codice dell'azione amministrativa* edited by M.A. SANDULLI, Milan, Giuffrè, 2017, sub art. 3-bis l. n. 241 of 1990, 519.

F. CARDARELLI, *Criteri di aggiudicazione*, in *Trattato sui Contratti Pubblici*, edited by M.A. SANDULLI and R. DE NICTOLIS, Milan, Giuffré,2019, 564.

F. CARDARELLI, *La motivazione del provvedimento,* in *Codice dell'Azione Amministrativa*, edited by M.A. SANDULLI, Milan, 2016, 397.

E. CARLONI, *Algoritmi sulla carta. Politiche di digitalizzazioen e trasformazione dgitale delle amministrazioni*, in *Dir. pubbl*., 2, 2019, 363 ff.

E. CARLONI, *La riforma del Codice dell'AMministrazione digitale*, in Giorn. dir. amm., 2011, no. 5, 469.

E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm*., 2, 2020, p. 281.

B. CAROTTI, *Sicurezza cibernetica e Stato-nazione,* in *Giorn. Dir. Amm*., 5, p. 629.

G. CARLOTTI, *I principi nel codice dei contratti pubblici: digitalizzazione*, in giustizia-amministrativa.it, 2023.

G. CARULLO, *Principio di neutralità tecnologica e progettazione* dei *sistemi informatici della pubblica amministrazione,* in *Cib. Dir.*, 1/2020.

M. CARTABIA, *La tutela multilvello dei diritti fondamentali. Il cammino della giurisprudenza della Corte Costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona*, in cortecostituzionale.it, 2014.

L. CASINI, *Lo Stato nell'era di Google,* Milan, Mondadori, 2020.

L. CASINI , *Lo Stato (Im)mortale. I pubblici poteri tra globalizzazione ed era digitale,* Milan, 2022.

S. CASSESE, *I beni pubblici. Circolazione e tutela*, Milan, Giuffre`, 1969.

S. CASSESE, *L'Arena pubblica. Nuovi paradigmi per lo Stato*, in *Riv. trim. dir. pubbl.,* 3, 2001, p. 601.

C. CATARISANO, *Commento sub. Art.* 108, in *Codice dei contratti pubblici annotato*, edited by L.R. PERFETTI, 829.

R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm*, 2, 2020, 305 ff;

R. CAVALLO PERIN, *Pubblica amministrazione e Big Data: da Torino un dibattito sull'intelligenza artificiale*, Turin, Quaderni del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino, 2021.

P. CERQUEIRA GOMES, *EU Public Procurement and innovation*, Cheltenham, 2021, p. 145; OECD, *Building Organization Capacity for Public Sector Innovation*, 2014.

P. CHIRULLI, *La partecipazione al procedimento*, in *Principi e regole dell'azione* amministrativa, edited by M.A. SANDULLI, Milan, 2023.

F. CINTIOLI, *Il principio di risultato nel nuovo codice dei contratti pubblici*, in www.giustizia-amministrativa.it

S. CIVITARESE MATTEUCCI, "*Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in *Dir. Pubbl*, 2019, p. 16.

M. CLARICH, *Prefazione*, in A. Lalli, *La pubblica amministrazione nell'era digitale*, Turin, Giappichelli, 2022, XIV.

M. CLARICH, *Il PNRR tra diritto europeo e nazionale: un tentative di inquadramento giridico*, July 2021, in *Corriere Giuridico*, no. 8-9/2021, 1025 ff.

M. CLARICH, *La disciplina del golden power in Italia e l'estensione dei poteri speciali alle reti 5g*, in G. NAPOLITANO (ed.), *Foreign Direct Investment Screening*, *il controllo sugli investimenti esteri diretti,* Bologna, il Mulino, 2019.

P. CLARIZIA, La digitalizzazione della pubblica amministrazione, in *Giorn. dir. amm.*, 2020, no. 6, 727.

P. CLARIZIA, *E-procurement*, in *The Digital State in the National Recovery and Resilience Plan*, Rome, 2022, 109 ff.

COGLIANESE-LEHR, *Trnasparency and Algorithmic Governance*, in *Administrative Law Review*, 2019, I.

C. COLAPIETRO-A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in *Le nuove frontiere della trasparenza nella dimensione costituzionale*, edited by C. COLAPIETRO AND L. CALIFANO, Editoriale Scientifica, Naples, 2014.

A. CORRADO, *Conoscere per partecipare: la strada tracciata della trasparenza amministrativa,* Naples, 2018.

A. CORRADO, *La trasparenza nella legislazione italiana*, in *Codice dell'azione amministrativa*, edited by M.A. SANDULLI, Giuffrè Editore, Milan, 2017.

A. CORRADO*, Il Principio di trasparenza e i suoi strumenti di attuazione*, in *Principi e regole dell'azione amministrativa*, edited by M.A. SANDULLI, Giuffrè Francis Lefevbre, 2020, p. 124

G. CORSO, *L'ordine pubblico,* Bologna, Il Mulino, 1979.

F. COSTANTINO, *L'uso della telematica nella pubblica amministrazione*, in *L'azione amministrativa* edited by A. ROMANO, Turin, Giappichelli, 2016, 242.

F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Dir. pubbl*., 1, 2019, pp. 43 ff.

F. COSTANTINO, *Gli open data come strumento di legittimazione delle istituzioni publbiche?*, in *Pubblica amministrazione con i big data da Torino un dibattito sull'intelligenza artificiale*, Turin, Quaderni del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino, 2021.

DESAI-KROLL, *Trust but verify: a guide to algorithms and the law*, in *Harvard Journal of Law & Technoloy*, 2017, 1.

D'AURIA, *Giannini and administrative reform*, in *Riv. Trim. dir. Pubbl.,* 4, 2000, 1209.

G. DELLA CANANEA, L. FIORENTINO (eds.), *I "poteri speciali" del governo nei settori strategici*, Naples, Editoriale Scientifica, 2020.

I.M. DELGADO, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?,* in *Ist. fed*., 3, 2019, pp. 643 ff..

V. DONATIVI, *Le società a partecipazione pubblica,* Milan, 2016.

E. ELIAM, *Reversing: Secrets of Reverse Engineering*, Wiley, 2011.

Z. ENGIN-P. TRELEAVEN, *Algorithmic Governance: Automating Public Services and Supporting Civil Servants in using Data Science Technologies*, in *The Computer Journal*, Vol. 62, No. 3, 2019.

V. FANTI, *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margin di una recente sentenza della Corte Costituzionale (n. 20/2019)*, in *Federalismi*, 5/2020.

M.R. FERRARESE, *Poteri nuovi,* Bologna, Il Mulino, 2023.

L. FLORIDI, *La Rivoluzione dell'informazione*, Turin, Codice Edizioni, 2012.

S. WACHTER-B. MITTELSTADT-L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, (December 28, 2016), in *International Data Privacy Law*, 2017, Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469.

G. FONDERICO, *I soggetti: stazioni appaltanti e operatori economici*, in *Il nuovo corso dei contratti pubblici. Principi e regole in cerca di ordine*, edited by S. FANTINI and H. SIMONETTI, Milan, 2023.

I. FORGIONE, *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni , tra regolazione europea e interna*, *Dir. Amm*, 4, 2022, 1114.

E.N. FRAGALE, Cittadinanza *amministrativa al tempo della digitalizzazione*, in *Dir. amm*., 2, 2022, 501.

F. FRANCARIO - M.A. SANDULLI, *Principio di ragionevolezza delle decisioni giurisdizionali e diritto alla sicurezza giurdica,* Editoriale Scientifica, Naples, 2018.

C. FRANCHINI, *L'organizzazione*, in S. Cassese (ed.), *Trattato di diritto amministrativo*, I, Milano, Giuffré,2003, 297 ff..

D.U. GALETTA-CORVALAN, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in Federalismi, 3/2019.

D.U. GALETTA-R.CAVALLO PERIN *Il diritto dell'Amministrazione Pubblica digitale*, edited by, Turin, Giappichelli, 2020.

D.U. GALETTA, *Transizione digitale e diritto ad una buona amministrazione fra prospettive aperte per le Pubbliche Amministrazioni dal PNRR e problemi ancora da affrontare*, in *Federalismi*, 7, 2022.

D.U. GALETTA, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione*, in *Riv. it. dir. pubbl. com.,* 3-4, 2005, 819 ff..

D.U. GALETTA-J. ZILLER (Eds.), *Information and Communication Technologies Challenging Public Law*, *beyond Data Protection*, Nomos Verlagsgesellschaft, 2018.

D.U. GALETTA, *Il principio di proporzionalità*, in M.A. SANDULLI, *Codice dell'Azione Amministrativa*, Milan, Giuffré, 2017, 149 ff.

W.V. GERVEN, *The European Union a polity of States and Peoples,* Stanford University Press, California, 2005.

C.GINTER-N.PARREST-M.A.SIMOVART, *Access to the content of public procurement contracts: the case for a general EU-law duty of disclosure*, in *Public Procurement Law Review*, 2013, 4.

A. GIORDANO, PANZAROLA, POLICE, PREZIOSI, PROTO in *Il diritto nell'era digitale*, edited by, Milan, 2022.

Y.N. HARARI, *Homo Deus, breve storia del futuro*, Milan, Bompiani, 2018.

N. IRTI, *Lo Stato: machina machinarum*, in *Riv. Trim. Dir. Pubbl*., 2004, 309.

D. JANČIĆ, *Transatlantic Regulatory Interdependence, Law and Governance: The Evolving Roles of the EU and US Legislatures*, in Cambridge Yearbook of European Legal Studies, 17 (2015), pp. 334–359

H. KELSEN, *Lineamenti di dottrina pura del diritto,* Piccola Biblioteca Einaudi, Turin, 1952.

A. LALLI, *L'Amministrazione pubblica nell'era digitale*, Turin, Giappichelli, 2022.

A. LALLI, *Introduzione*, in A. LALLI, *La pubblica amministrazione nell'era digitale,* Giappichelli, Turin, XVI.

LAWRENCE J. TRAUTMAN, MOHAMMED T. HUSSEIN, LOUIS NGAMASSI AND MASON J. MOLESKY, *Governance of the Internet of Things (IoT)*, in Jurimetrics Journal of Law, Science and Technology (Vol. 60, Issue 3), 2020.

F. LAVIOLA, E. CREMONA, V. PAGNANELLI. *Il valore economico dei dati personali*, Turin, 2022.

A. LICASTRO, *La riscoperta del'abuso di dipendenza economica nell'era dei mercati digitali*, in *Federalismi*, no. 13/2021, 118 ff..

M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, in *AIDA*, 2018, 199; SCHWARTZ, *Data processing and Government Administration: The Failure of the American Legal Response to the Computer*, in Hastings L.J., 1992.

MANGANARO, *L'evoluzione del principio di trasparenza amministrativa,* in *Astridonline.it*, 2009.

B. MARCHETTI, Voce *Amministrazione Digitale,* in *Enciclopedia del Diritto*, Milan, 2022, 76.

D. MARONGIU, *Aloritmi e procedure amministrative: una ricostruzione*, in Giur. It., 2022, 1520.

MARY C. LACITY-RUDY HIRSCHHEIM, *Information systems outsourcing; Myths, Metaphors and Reliabilities*, John Wiley & Sons Ltd, England, 1993.

A. MASUCCI, *L'atto amministrativo informatico*, Naples, 1993.

A. MASUCCI, *Digitalizzazione dell'amministrazione e servizi publbici "online". Lineamenti del disegno normativo*, in *Diritto Pubblico*, no. 1/2019, 124.

A. MASUCCI, *Vantaggi e rischi dell'automazione algoritmica delle decisioni amministrative*, in AA.VV., *Scritti in onore di Eugenio Picozza,* Vol. II, Naples, 2019, pp. 1105 ff..

A. MASUCCI, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, in *Dir. pubbl.,* 3, 2020, pp. 943 ff..

M. MATASSA, *La regolazione della cybersecurity in Italia*, in *La sicurezza nel cyberspazio*, edited by R. URSI, Franco Angeli, Milan, 2023.

M. MAZZUCCATO, *Lo Stato innovatore*, Bari, 2014.

S. MELE, *Il perimetro di sicurezza nazionale cibernetica e il "nuovo" golden power*, in *Il diritto di internet nell'era digitale*, edited by S. PREVITI and G. CASSANO, Milan, Giuffré, p. 186.

M. MONTEDURO, *I principi del procedimento nell'esercizio del potere sanzionatorio delle Autorità amministrative indipendenti*. *Tessuto delle fonti e nodi sistematici*, in ALLENA-CIMINI (ed.), *Il potere sanzionatorio delle Autorità amministrative indipendenti*, in *Il diritto dell'economia*, 2013.

M.J. MORRISON, *The acquisition supply chain and the security of Governement information technology* purchases, in Public Contract Law Journal , 42, 4, 2013, 749-792.

C. MIRABELLI*, Il rischio da diritto. Il costo dell'incertezza ed alcune possibili economie*, in *La certezza del diritto - Un valore da ritrovare - Atti del convegno*, Firenze, 2-3 ottobre 1992, Milano, 1994, 39.

M. MIRRIONE, *La selezione delle offerte*, in *Il nuovo corso dei contratti pubblici. Principi e regole in cerca di ordine*, edited by S. FANTINI and H. SIMONETTI, Il Foro Italiano-Gli speciali, 2023, no. 1, 146 ff.

G. MORBIDELLI, *Il principio di legalità e i cd poteri impliciti*, in Dir. amm., 2007, 4, 703 ff.

G. MORBIDELLI, *Codice delle Società a partecipazione pubblica*, edited by, Milan, 2018.

G. NAPOLITANO, *Il partenariato public-privato per l'implementazione del Polo Strategico Nazionale* in *Giorn. Dir. Amm.*, 6/2021, 703-707.

G. NAPOLITANO (ed.), *Foreign Direct Investment Screening, il controllo sugli investimenti esteri diretti,* Bologna, il Mulino, 2019.

G. NAPOLITANO, *L'irresistibile ascesa del golden power e la rinascita dello Stato doganiere*, in *Giorn. Dir. Amm.,* no. 5, 2019, p. 551.

A. NATALINI, *Come il passato influenza la digitalizzazione della pubblica Amministrazione*, in *Riv. trim. dir. pubbl.,* no. 1, 2022, 95.

L. NELVILLE BROWN - T. KENNEDY, *The Court of Justice of the European Communities,* Sweet and Maxwell, London, 2000, p.2 et seq.

V. NERI, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in Urb. and App., 2021, 5, 581.

F. NASSUATO, *Legalità algoritmica nell'azione amministrativa e regime dei vzi procedimentali*, in *Ceridap*, 1, 2022, 151.

L. OLMSTED, The Amazon-ization of Federal Procurement: using the Uniform Commercial Code to moderate an inevitable innovation, in *Public Contract Law Journal,* 28, 1, 2018, 101-122.

A.G. OROFINO, *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in Foro amm. C.d.S., 9, 2002, pp. 2256 ff..

A.G. OROFINO, G. GALLONE, *Intelligenza artificiale al servizio della funzione amministrativa: profili problematici e spuinti di riflessione*, in *Giur. it*., 7, 2020, pp. 1738 ff..

P. OTRANTO, *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, in Federalismi.it, 7, 2021.

G. PALMISANO, *Il Sistema giuridico internazionale e l'ordinamento comunitario, 2012,* in *treccani.it*.

N. PAOLANTONIO, *Il potere discrezionale della pubblica automazione. Incertezze e stilemi*, in *Dir. amm*., 4, 2021, pp. 813 ff..

G. PASCUZZI, *Il diritto dell'era digitale,* Il Mulino, Bologna, 2020.

F. PATRONI GRIFFI, *La giustizia Costituzionale in trasformazione: La Corte Costituzionale tra Giudice dei diritti e Giudice dei conflitti,* in Federalismi, 20, 2011.

S. PERONGINI, *Il principio del risultato e il principio di concorrenza*, in Dir. e soc, 2022, 3, 551 ff..

E. PLAS, *Amendements tu public contracts: in searcg of a sufficient degree of transparency*, in *Public Procurement Law Review*, 2021, 1.

A. POLICE, *Scelta discrezionale e decisione algoritmica*, in *Il diritto nell'era digitale*, edited by GIORDANO, PANZAROLA, POLICE, PREZIOSI, PROTO, Milan, 2022, 496.

O. POLLICINO, *Digital Power*, in *Encyclopedia of Law*, *Thematics*, V - 2023, 410 ff..

L. PREVITI, *Pubblici poreri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi*, no. 25/2022.

R. PROIETTI, *La partecipazione al procedimento amministrativo,* in *Codice dell'azione amministrativa*, edited by M.A. SANDULLI, Milan, 2017, 566.

S. PUGLIATTI, *Voce Diritto Pubblico e diritto privato*, in *Enciclopedia del* diritto, Milan, 1964, XIII, p. 696.

G.M. RACCA-R.YUKINS, *Joint Public Procurement and Innovation,* Brussels, 2019.

G.M. RACCA-R. CAVALLO PERIN-G.L. ALBANO, *Competition in the execution phase of public contracts*, in *Public contracts Law Review*, Cl. 41, no. 1, 2011, p. 99-103.

B. RAGANELLI, *Decisioni pubbliche e algoritmi: modelli di dialogo nell'assunzione di decisioni amministrative*, in Federalismi.it, 22, 2020.

A. RENZI, *La sicurezza cibernetica: lo stato dell'arte*, in *Giorn. Dir. Amm.*, 4, 538.

S. ROSSA, *Cybersecurity e pubblica amministrazione,* Naples, Editoriale Scientifica, 2023.

D. SABATINO, *Contratti della difesa e contratti secretati*, in *Trattato sui contratti pubblici*, edited by M.A. SANDULLI and R. DE NICTOLIS, Milan, Giuffré, 2019, IV, 923 ff..

F. SAITTA, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, in *Riv. dir. amm. elettr*., 2003, pp. 24 ff..

A.M. SANDULLI, *Beni pubblici,* in *Enc. dir.*,V, Milan, Giuffre`, 1959.

M.A. SANDULLI, *I Principi costituzionali e comunitari di giurisdizione amministrativa,* in *Il nuovo processo amministrativo,* edited by M.A. SANDULLI, Giuffrè Editore, Milan, 2013, p. 29.

M.A. SANDULLI, *Prime considerazioni sullo scema del nuovo codice dei contratti pubblici*, in Giustiziainsieme.it, December 21, 2022.

M.A. SANDULLI, *Il ruolo dei principi nel diritto amministrativo. Introduzione a Principi e Regole dell'azione amministrativa – Quarta Edizione 2023*, in www.giustiziainsieme.it.

M.A. SANDULLI, *Principi e regole dell'azione amministrativa. Riflessioni sul rapport tra legge e realtà giurisprudenziale*, in *Federalismi*, no. 23/2017.

M.A. SANDULLI, *Conclusioni ad un dibattito sul principio alla certezza del diritto*, in *Principio di ragionevolezza delle decisioni giurisdizionali e diritto alla sicurezza giuridica*, edited by F. FRANCARIO and M.A. SANDULLI, Naples, 2018, 305.

A. SANDULLI, *Pubblico e Privato nelle Infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513.

A. SANDULLI, *La febbre del golden power*, in *Riv. Trim. Dir. Public,* 3, 2022, 743.

F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi*, 12/2022.

A. SIMONCINI, *Profili costituzionali dell'amministrazione algoritmica*, in *Riv. trim. dir. pubbl.,* 4, 2019, pp. 1149 ff..

M.A. SIMOVART, *Old remedies for new violations? The deficit of remedies for enforcing public contract modification rules*, in *UrT*, 2015/1, pp 33-47.

A. SOLA, *Inquadramento giuridico degli algoritmi nell'attività amministrativa*, in Federalismi.it, 16, 2020.

M.R. SPASIANO, *Il principio del buon andamento*, in *Codice dell'Azione Amministrativa*, edited by M.A. Sandulli, Milan, 2017.

M.R, SPASIANO, *Nuovi approdi della partecipazione procedimentale nel prisma del novellato preavviso di rigetto*, in *Diritto dell'economia*, 2022, 30.

M.R. SPASIANO, *Principi e discrezionalità nel nuovo codice dei contratti pubblici*: *primi tentativi di parametrazione del sindacato*., in federalismi.it, 2023, no. 24, 222.

M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds & Machine*, 2019, 9.

G. TESAURO, *Diritto dell'Unione Europea,* Cedam, Padova, 2012.

S. TRANQUILLI, *Il rapporto pubblico-privato nell'adozione e nel controllo della decisione amministrativa "robotica",* in *Dir. soc*., 2, 2020, pp. 281 ff..

F. TURATI, *Discorsi parlamentari,* Camera dei Deputati, Sessions 1904-1908, June 17, 1908, 22962.

F. TRIMARCHI BANFI, *Il diritto ad una buona amministrazione*, in M.P. CHITI, G. GRECO (eds.), *Trattato di diritto amministrativo europeo. Parte generale*, Tomo I, Milan, 2007, 49 ff.

L. TORCHIA, *Lo Stato Digitale. Una Introduzione,* Bologna, Il Mulino, 2023.

R. URSI, *La sicurezza pubblica*, Bologna, Il Mulino, 2022.

R. URSI, *Cybersecurity come funzione pubblica*, in *La sicurezza nel cyberspazio*, edited by R. URSI, Franco Angeli, Milan, 2023, pp. 17.

L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Federalismi*, 21, 2018.

L. VIOLA, *Attività amministrativa e intelligenza artificiale,* in *Cib. dir.,* 1-2, 2019, pp. 64 ff..

F. ZACCARIA, *La perdita della certezza del diritto: riflessi sugli equilibri dell'economia e della finanza pubblica*, Pavia, 2003.

A. ZITO, *Il "diritto ad una buona amministrazione" nella Carta dei Diritti Fondamentali dell'Unione Europea e nel diritto interno*, in *Riv. it. dir. pubbl. com*, 2, 2002, 425 ff..

A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020, 56.