Legal Technology Transformation

A Practical Assessment

Edited by

Andrea Caligiuri

Editoriale Scientifica

2020

Legal Technology Transformation
A Practical Assessment

Edited by
Andrea Caligiuri

EDITORIALE SCIENTIFICA

2020

Via San Biagio dei Librai, 39 – 80138 Napoli
www.editorialescientifica.com – info@editorialescientifica.com

ISBN 978-88-9391-985-2

SCIENTIFIC COMMITTEE

TABLE OF CONTENTS

Preface ………………………………………………………………………………..… 1

PART I
FREE MOVEMENT OF PERSONAL AND NON-PERSONAL DATA

Introduction ……………………………………………………………………………… 5
STEFANO VILLAMENA

1. New Technologies, Big Data and Human Rights: An Overview ………………………… 11
ARIANNA MACERATINI

2. Protection of Personal Data and Human Rights
between the ECHR and the EU Legal Order ……………………………………………... 21
ALFREDO TERRASI

3. Promoting a Common Understanding of the GDPR: European
Data Protection Board and National Data Protection Authorities ………………………… 33
MARCO MACCHIA

4. Protection and Trade of Non-personal Data …………………………………………… 40
CRISTINA RENGHINI

5. Protection of Personal and Non-personal Data:
A Chinese Perspective ……………………………………………...………………… 48
YUTING YAN

6. Digital Humanism between Ethics, Law,and New Technologies ………………….…. 65
MARIA CONCETTA DE VIVO

7. Labor Relations, Intelligent Machine, Digital Plants.
Legal Problem related to Data and Social Protection …………………………….…… 80
MICHELE FAIOLI

PART II
USE OF UNMANNED AERIAL, MARITIME AND GROUND SYSTEMS
IN CIVIL AND MILITARY FIELDS

Introduction ……………………………………………………………………..…..… 89
STEFANO POLLASTRELLI

1. Air Traffic Control by Satellite: Some Legal Aspects ………………..…………………. 91
SILVIO MAGNOSI

2. A New International Legal Framework for Unmanned Maritime Vessels? ……………. 99
ANDREA CALIGIURI

3. Connected and Automated Mobility of Road Vehicles ………………………………… 110
CARMEN TELESCA

4. The Ethical and Legal Implications of Autonomy in Weapons Systems ………….....…. 119
DANIELE AMOROSO, GUGLIELMO TAMBURRINI

PART III
ARTIFICIAL INTELLIGENCE AND SMART CITIES

Introduction ……………………………………………………………………………... 131
ALESSIO BARTOLACELLI, CHIARA FELIZIANI, FRANCESCA SPIGARELLI

1. Artificial Intelligence Applied to Cities …………………………………………….…. 133
EMANUELE FRONTONI, LUCA ROMEO

2. Electric Smart Grid …………………………………………………………………… 140
ALESSIA ARTECONI

3. Smart Cities and Airbnb: Platforms as 'Regulatory Intermediaries'
in Short-term Rental Market? ……………………………………………………….…. 147
GIACOMO MENEGUS

4. Technological Innovation and Artificial Intelligence Applied to
Intermodal Transport: The Case Study of the Port of Ancona …………………………… 154
MATTEO PAROLI

PART IV
LEGAL RAMIFICATIONS OF BLOCKCHAIN TECHNOLOGY

SECTION I
BLOCKCHAIN AND CRYPTOCURRENCIES

Introduction …………………………………………………………………………… 167
KONSTANTINOS SERGAKIS

1. The Economic Framework and
Applications of Blockchain (Distributed Ledger) Technology …………………………… 170
TAMIR AGMON, LEVY COHEN

2. Blockchain and Privacy: Can they Coexist? 181
MARCO BALDI, DALILA CALABRESE, GIULIA RAFAIANI

3. Blockchain and Criminal Risk 189
ROBERTO ACQUAROLI

4. Bitcoin and Cryptocurrencies. Tax Law Related Profiles 195
GIUSEPPE RIVETTI, PAOLA CRICCO

5. Blockchain and ICOs (A Sisyphean Juridical Tale on
Financial Markets and Innovation) 208
ALDO LAUDONIO

SECTION 2
BLOCKCHAIN AND LEGAL IMPLICATIONS
FOR PRIVATE LAW AND BUSINESS LAW

Introduction – The Blockchain Technology between
the Law of Contemporaneity and the New Power Structure 223
FRANCESCO GAMBINO

1. Blockchain Application in General Private Law: The Notarchain Case 229
ENRICO DAMIANI

2. Blockchain Applications and Company Law 237
FLORIAN MÖSLEIN

3. Anonymity and Pseudonymity. Fintech and the Key Issue of Traceability 245
ELISABETTA PEDERZINI

4. Blockchain and the Food Supply Chain: The Future of Food Traceability 260
PAMELA LATTANZI, SERENA MARIANI

List of Authors 269

PREFACE

The Digital revolution is the greatest transformative force in human history, and it is creating new challenges for legal systems across the globe. This revolution has defied the traditional tools that Jurists have at their disposal to study, evaluate and regulate social spaces. The latter are in fact subject to a rapid and continuous transformation that has an increasingly significant impact on the governance of national communities and international society.

Today, it is the hard task of Jurists to develop a new legal framework to take advantage of this rapid technological change so as to make the world more prosperous and inclusive.

The complexity and quantity of relevant topics in this area have led us to select the most significant issues for understanding the phenomenon of transformation of the law in the context of digitalization. Thus, the book is organized into four parts dedicated to the following subject-matters:

Part I – *Free Movement* of *Personal and Non-personal Data*

Part II – *Use of Unmanned Aerial, Maritime and Ground Systems in Civil and Military Fields*

Part III – *Artificial Intelligence and Smart Cities*

Part IV – *Legal Ramifications of Blockchain Technology*.

The areas were chosen among those in which technological innovation seems to be more challenging for the legal categories and institutions of public law, private law and commercial law at national, European and international level.

The main purpose of the book is to analyse the needs and requirements for the adaptation of traditional legal models of reference to address the challenges arising from the development and the use of digital technologies and their products. In this regard, a decision was made to take a practical approach in examining the different legal issues.

This book also seeks to combine the accuracy of scientific inquiry with a special attention to the necessities of teaching in order to offer a useful tool, not only to legal professionals, but also to university students who for the first time approach the study of these issues.

The contributions were written by highly qualified academics and scholars in their field of expertise from different European countries and China. My sincere gratitude goes to all of them.

Special acknowledgments go to the Institute of International Law of the Chinese Academy of Social Sciences as scientific partner in this editorial project and to the Department of Law, University of Macerata, that supported it within one of the initiatives implementing the "*Dipartimento di Eccellenza*" Project, entitled "Law and Innovation: Europe and China Facing the Challenges of Globalization", funded by the Italian Ministry of Education, University and Research.

Macerata, 20 December 2020

ANDREA CALIGIURI

PART I

FREE MOVEMENT OF PERSONAL AND NON-PERSONAL DATA

INTRODUCTION

STEFANO VILLAMENA

Part I of this book collects studies on the topic of freedom of circulation of personal and non-personal data. Moving in this wide-ranging research field, the seven authors carried out a transversal survey, investigating among the relationship between Big Data and human rights, the Protection of Personal Data and Human Rights in the European Convention on Human Rights (ECHR) and in the EU legal system, the regulatory authority for data protection at the national and euro-unit level, the regulation of the protection and trade of non-personal data, the regulation of personal and non-personal data according to Chinese legislation, the ethical aspects related to the regulation of artificial intelligence and Big Data and finally how digital technologies affect employment.

By looking at the relationship between Big Data and human rights, A. Maceratini highlights the role of Big Data in our society and their ability to produce knowledge. In fact, Big Data contains different types of data, starting from demographic data up to behavioral data, extrapolated from the entire population. These detect by virtue of their predictive effectiveness with consequent enhancement of the quantity rather than the accuracy of the analysis procedure. The significant aspect of predictions consequently implies the economic value of knowledge extraction techniques.

The author therefore raises the problem of the relationship between Big Data and Privacy, given the difficulty of establishing when and to what extent the user is aware of the collection of personal data by companies that provide an information service. The problem concerns the imbalance of power between the company providing the services due to the indispensability of them and the user who is led to consent to the release and use of data compromising the self-determination to the processing of data. It should be noted that the problem mentioned is relevant in terms of Big Data since, although they are anonymous data, with appropriate correlations it is possible to refer them to very specific people.

For this reason, we need a European discipline that looks at this aspect. On the self-determination side, the author shows the Big Data problem regarding the individual profiling, especially by Big Tech, which creates a filter bubble aimed at showing the user the information that the algorithm has decided as potentially interesting for him. To guarantee the self-determination of the person, it is necessary to insert procedural mechanisms of transparency that guarantee the knowledge of the automated decision-making process and the explainability of the results, so as to guarantee a balance between freedom of economic initiative and protection of confidentiality.

A. Terrasi analyzes the relationship between the protection of personal data and human rights comparing the ECHR and the EU legal protection. The author highlights the absence of a legal framework on data protection in human rights treaties, including the ECHR, because they were born before the notion of personal data so he analyzes the tools drawn up by the Council of Europe to guarantee data protection. A critical examination of ECHR case law shows that is possible to recognize a data protection through the application of Art. 8 of the Charter even if nothing is provided on personal information. The paper continues by analyzing the case-law of the Court of Justice of the European Union (CJEU) on data protection regarding the application of Articles 7 and 8 of the Charter of Nice. In order to understand the relationship between Art. 7 and Art. 8 of the Charter of Nice on data protection and cross-border flows, the author examines several rulings concerning Google and Facebook.

Moving on to the topic of regulatory authorities for data protection, M. Macchia puts at the center of its work the importance of the regulation and supervision of the European Data Protection Board (EDPB) in relation to the collection of data by political parties which, through the use of behavioral techniques, send targeted electoral messages. For the General Data Protection Regulation 679/2016 (GDPR), data that reveals political opinions are a special category. This requires the transparency of the sending processes in which the voter must be made aware of why he is receiving a message from a political party, as this conduct is potentially harmful to democracy, so as to preserve the integrity of the elections and the citizens 'trust.

To reduce the risks linked to processing personal data for political purposes, the EDPB collaborates with the national authorities of the member states to ensure conduct compliant with the GDPR and a uniform interpretation on the territory of the European Union.

The authorities have the task of monitoring the application of supranational rules, also ensuring through coherence and collaboration mechanisms uniform levels of protection in the territory of the member states.

The author therefore highlights the relationship between national authorities and between national authorities and the EDPB, underlining that the GDPR safeguards the independence of authorities by indicating the tasks and powers of domestic data protection authorities. Investigating the reasons for the choice of the EU legislator, the mechanisms of connection between national authorities are examined: cooperation and the coherence mechanism.

As for the first, the cooperation between data protection authorities of the Member States is required by the law of the European Union and operates when the data processing is cross-border. In this case the EDPB has a supervisory role.

On the other hand, in the event of a conflict between authorities regarding the application of the data processing discipline, the consistency mechanism operates in which the EDPB, having received the draft decision, formulates an opinion on the matter by a majority of its members.

The author underlines that the outlined system of European data protection confirms a vertical independence of national decision makers, in contrast to other processes of European integration.

On the subject of the protection and trade of non-personal data, C. Renghini, aware of how data today is a great source of wealth, first takes care of distinguishing non-personal data from personal data according to European legislation and then defines the circulation methods of non-personal data through the analysis of the new regulation on the free flow of non-personal data and the relevant directives (Regulation (EU) 2018/1807, FFD).

With regard to the first point, it should be noted that the definition of non-personal data is extracted from the Art. 4 GDPR has the opposite definition of personal data. Thus, a broad and flexible notion of non-personal data is determined, with the consequence that everything could fall within the field of personal data given the wide interpretation of this notion. Next, the notion of anonymous data is examined. The anonymous data contains information that cannot be related to an identified or identifiable person from the beginning. The pseudonym data instead can be correlated to a person using additional information. The author highlights two different interpretations to define whether a given pseudonym is personal. The first interpretation, relating to Recital 26 of the GDPR, adopts a risk-based approach, when identification is not reasonably probable taking into account objective factors. The second interpretation refers to the Opinion 05/2014 on the techniques of anonymization where Art. 29 Data Protection Working Party (WP29) shows that the process of transformation into anonymous form must reach an "irreversible de-identification". Consequently, the correct anonymization of data depends on the specific circumstances of each individual, making it difficult to understand the legal regime of application between the GDPR for personal data and the FFD regulation for non-personal data. In the event of coexistence in the same dataset of personal and non-personal data, the application of the GDPR is emphasized if the data are not "inextricably linked" while in the event of a split the FFD regulation will apply to personal data. Although there is no notion of "inextricably linked", the author tries to define it.

Then, article examines the content of the FFD regulation aimed at guaranteeing the free flow of non-personal data within the European Union, considered the fifth freedom on the single market to complement the four traditional ones such as persons, goods, services and capital. In this context, the paper highlights the limitations defined by the Commission on the location of data for storage or processing and then underlines the breadth of the definition given of the data location requirements and the defining role of the CJEU. The article continues to examine the only exception that the FFD regulation provides for the free- flow of data, that is, "the data localization requirements are prohibited unless they are justified for reasons of public safety in compliance with the principles of proportionality". At the center of the analysis is the need to investigate Art. 52 TFEU and the case law of the CJEU to establish the scope of the exception. The author emphasizes the necessary compliance with the FFD regulation of EU law through the provision of a predefined cooperation mechanism between competent authorities in the matter and outlines that the regulation encourages the adoption of codes of conduct at the European level to introduce good practices to facilitate the change of supplier and guarantee adequate information to professional users before the conclusion of a contract for the storage and processing of data.

The article ends with the analysis of the rules on legal protection and data trade not covered by the FFD regulation. In this part, the paper notes that the current law does not provide for specific rights on data, subsequently examining in detail the unsatisfactory regime of the laws concerning intellectual property rights, the protection of databases (Directive 96/9/CE) and the rules on trade secret (Directive (EU) 2016/943). The need to create a new propriety right of data is therefore affirmed without neglecting the problems that could arise from this novelty.

Moving on to the analysis of the discipline of personal and non-personal data according to Chinese legislation, Yuting Y. introduces his theme by recalling the universal information revolution that derives from the introduction of Big Data technology and artificial intelligence technology, raising concerns about safeguarding the human rights of vulnerable groups by virtue of the frequent automatic discrimination of Big Data and the erosion of the right to privacy. Given China's position as a world leader in technology and data volume, the author examines its data governance and safeguarding system based on national conditions. To this end, the paper examines the necessity accepted by China to regulate data protection in a differentiated manner, highlighting the difficult balance between the protection of personal rights and interests incorporated in data and the economic value of data as a resource and the consequent gaps in the relevant laws. The author focuses on the different discipline of personal data that does not find a specific definition, unlike what happens in the European discipline in Art. 4 GDPR. In China, personal data is data that alone or in combination with other data can identify a specific natural person, moving from an initial concept of "personal information" to "personal data".

The evolution of the legal terminology of "personal data" is highlighted through the analysis of the Constitution of the People's Republic of China up to the recent Cybersecurity Law, recognizing an initial desire to protect data as a legal object. This will in China is represented by the development of new data rights, recognized through the Personal Data Protection Act in a separate Personal Data Protection legislation. Non-personal data, on the other hand, which includes corporate data and government data, are often associated with important and sensitive data with the consequent need to submit them to a regime for the management of cross-border data movements. This article then continues with the examination of data protection mechanisms under Chinese legislation which follows a value-oriented approach of placing equal emphasis on security and development, balancing the protection of human rights and the effective use of data and promotion, development, data sharing.

The author therefore reviews the rules concerning the aspects indicated with reference to both the management of cross-border movements of personal data to maintain social stability and the effective use of data, both to personal data protection for children, and to the system management of important and sensitive data and the law on data security. The paper does not neglect China's draft concerning the introduction of the data security law drafted in order to find a balance between "data security and effective use", giving equal emphasis to development and security. This draft deals with regulating three relationships: the first is the relationship between the State, businesses and individuals in the context of data security obligations; the second is the horizontal and vertical relationship in the data protection mechanism and finally the third is the relationship between regulator and supervisor.

Then, the author examines the current situation of data protection legislation because the competitiveness of the Chinese data economy industry increases in recent years. National legislation on corporate data protection is shown which increasingly tends to clarify the boundaries between data exploitation and data protection in cases of data breach, so as to build a good national image of data protection compared to the past and ensure international cooperation on cross-border data movements.

A great role for the implementation of data protection discipline comes from the self-regulation of the data industry promoted and initiated by regulators and consumer associations under the guidance of laws and regulations. The paper therefore examines such practices, reporting recent cases of Chinese digital enterprises now serving as a vehicle for formulating relevant international standards.

Having analyzed the criticalities of the Chinese regulation on differentiated data protection, the paper explores current trends of the Chinese legislation.

China is currently promoting the construction of a complete, reasonable and balanced system of data governance based on the consensus among all stakeholders, of an institutional and legal system for differentiated data governance and coordinating the relationship between government, businesses and users in the use of data which has its basis in data protection. In addition to this, China is implementing a pilot zone for digital commerce for the employment of a free cross-border movement of data.

The paper ends with the author's critical analysis of the Chinese system, recalling the need for better coordination of public and commercial interests and the introduction of a multi-subject governance system that passes from a "protection of personal information" to "Govern the data". Furthermore, the author affirms that China cannot disregard a logic of internal cooperation between government and companies linked to cross-border activities to ensure an adequate guarantee system at the state level for cross-border data movements. A cooperation that must also take on international connotations to promote multilateral negotiations on cross-border data movements and the creation of frameworks for international law enforcement collaboration on data issues.

About the ethical aspects related to the discipline of artificial intelligence and Big Data*,* M. C. De Vivo introduces his work highlighting that by virtue of technological innovations we are facing a digital humanism characterized by a "digital world" in which man lives and carries out his activities. This world carries the risk of an "erosion" of decision-making autonomy influenced by the pervasiveness of new technologies that impose certainties and security to be guaranteed through law and ethics. The author underlines how the large amount of data they pour into society can be traced back to Big Data that have different nature, origin and content (photos, videos, voice messages and data in applications). Although these data appear neutral, they have an economic significance, hiding an attractive potential to be brought out through a sophisticated algorithm capable of bringing out predictive knowledge useful to society in all sectors. Since it is easy to abuse this potential, it is necessary to reserve a protection for this data. In fact, even if Big Data is anonymous, it is possible to identify the data subject through the processing of data. The author highlights the inadequacy of the regulation of the GDPR which, dealing only with personal data, is inadequate to protect the interested parties involved in Big Data that contain personal data and not. Their management is carried out by complex and cryptic algorithms that are not compatible with the transparency of the GDPR discipline. Moreover, they are collected indiscriminately, without any prior planning, making control difficult. Finally, on this point, the nature attributed to Big Data databases is criticized and the indications coming from the privacy guarantor are reported to the legislator in which the main problems of protection of interested parties regarding Big Data are highlighted. This paper subsequently underlines the need to resort to "special protections" such as Ethics and Law to address technological progress. In fact, even if the algorithm is based on an automatic procedure, it cannot be defined as neutral as the algorithm represents human opinions embedded in the mathematical language.

For this reason, it is necessary to make ethics and law coincide also in order to guarantee fundamental rights. Finally, the work analyzes the notion of artificial intelligence and then reviews the European and Italian discipline on the subject from which the desire to aim for ethical development for reliable artificial intelligence is inferred. The author also examines the type and nature of the responsibility that could concern artificial intelligence by distinguishing the hypotheses of non-agent AI and agent AI, the latter being equated to a sentient subject. To assess possible criminal liability under the application of Art. 27 of the Italian Constitution an accurate analysis is reserved to this type of artificial intelligence.

Part I of this book ends with the paper of M. Faioli which analyzes how new digital technologies affect employment. The author points out that the intelligent machine can be considered a third element that takes part in the legal issues of the contractual pattern involving the employer and the worker. In this way the organization of work is changing with a consequent modification of the legal provisions and collective bargaining that adapt to the novelty. This paper also highlights how these changes break the Fordist paradigm. Then, the author questions whether collective bargaining encounters limits in this area of protection, underlining the ability of collective bargaining itself to anticipate needs and address problems beyond the applicable legislation. This article investigates the possibility of considering the object of the employment contract integrated by the monitoring and regulatory action carried out by intelligent machines, thus replacing the employer. This problem arises in reference to machines that have deep learning, replacing men in the exercise of their duties and coordinating them through a process of self-determination. The author explains that this situation will significantly change not only the organization of work but also the concept of job, employment contract and notion of employer, proposing in this article a methodology aimed at outlining a theory of job duties in an industrial world under pressure of the intelligent machine that sees collective bargaining at the center to ensure fair interaction between machine and man observing the law.

NEW TECHNOLOGIES, BIG DATA AND HUMAN RIGHTS: AN OVERVIEW

ARIANNA MACERATINI

SUMMARY: 1. Big Data in the Information Society. – 2. Big Data. – 3. Big Data and Privacy. – 4. Big Data and Information.

1. *Big Data in the Information Society*

In the new economy, information is a fundamental economic resource that optimizes the relationship between supplier and user, for the loyalty of the latter.[1] The delineation of individual profiles and preferences will, in turn, contribute to influencing subjective behavior as significantly demonstrated by the phenomena of anticipatory shipping and anticipatory selling, developed by Amazon, capable of anticipating and inducing, apparently without forcing, the future customer purchases.[2] In this direction, also indicated by Opinion 8/2014 on the Recent Development on Internet of Things of Article 29 Data Protection Working Party (hereinafter "WP29"),[3] it is evident that the pervasiveness of information technologies, mainly of the Internet of Things,[4] has facilitated digital surveillance practices, making anyone who uses a computer device connected to the network easily

[1] J. Rifkin, *L'era dell'accesso* (Mondadori 2001), 65.

[2] D. Talia, *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale* (Rubettino 2018) 25.

[3] WP29, Opinion 8/2014 on the Recent Developments on the Internet of Things, WP223, 16 September 2014. On this argument, S. Palanza, *Internet of things, big data e privacy: la triade del futuro* (IAI 2016) 18 ff.

[4] The Internet of Things (hereinafter "IoT"), an expression coined by the British researcher Kevin Ashton in 1999, expresses the transition from a network of interconnected computers to a network of connected everyday objects, facilitated by the development of wireless and satellite technology, see Palanza (n 3), 2. The identification of interconnected objects occurs mostly through a unique identifier, recognizable in radiofrequency, M. Iasselli, 'Privacy e nuove tecnologie', in M Iasselli (ed.), *Diritto e nuove tecnologie. Prontuario giuridico ed informatico* (Altalex 2016) 121 ff., 153 ff. Radiofrequency identification (hereinafter "RFID") is based on the use of microprocessors connected to an antenna, used as identification labels – *intelligent labels* – and capable of transmitting, via radio waves, signals readable by special readers; see ibid., 135. It should be noted that RFID has recently been joined by the massive use of Near Field Communication (hereinafter "NFC"), technologies that provide two-way and short-range wireless connectivity; see Palanza (n 3). On the impact of RFID on the exercise of individual freedom rights and on the protection of personal data involved in this kind of electronic processing, the European Data Protection Supervisor (hereinafter "EDPS") had already pronounced with an opinion of 20 December 2007 concerning the guarantees in the use of smart labels (EDPS, 'Opinion on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework (COM(2007) 96)', 20 December 2007), as well as the Commission of the European Communities with the Communication 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework', COM(2007) 96 final, 15 March 2007, outlining a political line that has as its objective the difficult reconciliation between the enhancement of the technologies and the protection of privacy, underlining the risks to health and the environment deriving from their use.

traceable and monitored by dealing – in some cases even without the data subject being aware of it, for example due to a sudden activation of the device used[5] – personal data, including information of a sensitive nature which, at a later time, could be aggregated to others allowing a more or less defined profiling of the interested party.[6] In fact, it should be noted that the data analyzed individually may not be particularly significant, but, if examined with suitable information technologies and in large volumes, they lead to the delineation of models and trends, capable of producing knowledge. It is therefore possible to intend how the term "personal data" is to be understood, following the direction of the 2013 OECD Guidelines[7] in an evolutionary and extensive key.[8] In any case, the massive processing of information marks the transition from a purely individual dimension of personal confidentiality to a collective dimension of the protection of personal data, in which the subject of informative self-determination becomes the entire community,[9] in the firm resolution to subtract from exclusive domain of the market information that constitute and guard the core of fundamental rights.[10]

2. *Big Data*

In the aforementioned OECD definition, all content generated by users on the Internet is Big Data, including blogs, photos, videos, behavioural data, social data, geolocation data, demographic data and identification data in general: contents that allow individual identification or which provide information on typed patterns of

[5] Palanza (n 3), 15.

[6] Iasselli (n 4), 135. In Italy, the regulation of the protection of personal data is contained in the Legislative Decree No. 196/2003, Privacy Code, aimed at bringing together the innumerable provisions of the sector which have occurred over the years and at introducing the most significant innovations of the Italian Data Protection Authority and of the European Directives on the confidentiality of electronic communications. Among the latter, it is necessary to mention the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, a provision recently repealed by General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR"); Legislative Decree No. 101/2018 adapted the Privacy Code to the provisions of GDPR. The current meaning assumed by privacy, by individualistic and substantially passive protection of the right to be left alone with the right to full control of information concerning us, is also sanctioned by the Charter of Fundamental Rights of the EU, which in Art. 8 provides for the right to the protection of personal data, as well as the Italian Declaration of the Internet Rights, published on 13 October 2015 during an international conference held at the Sala della Regina in Palazzo Montecitorio, S. Rodotà, *Il mondo nella rete* (Laterza 2012) 31.

[7] OECD Guidelines governing the protection of privacy and transborder flows of personal data (2013) <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. See Palanza (n 3), 8. It should be noted that the *ePrivacy Regulation* proposal of the European Commission (COM/2017/010 final – 2017/03 (COD), 10 January 2017) included in the category of metadata all data other than content, but only those processed on the network and not also data processed on devices, as also noted by the European Data Protection Supervisor, 'Opinion 6/2017 – EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)'.

[8] M. Orefice, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica* (Aracne 2018) 100.

[9] M. F. De Tullio, 'La privacy e i big data verso una dimensione costituzionale collettiva' (2016) Politica del diritto 641.

[10] Orefice (n 8), 141.

individual behaviour.[11] Big Data can also be described by means of the so-called 4Vs, that is, *volume*, as they are present in large quantities; *variety*, as they come from heterogeneous sources; *velocity*, since the data is analyzed through sophisticated algorithms that lead to a decision in real time;[12] *value* assumed, in this way, by the data.[13] It should be noted that most of this data is usually unstructured, that is, acquired and stored according to criteria different from those that oversee the organization of traditional electronic archives:[14] the peculiarity and potential of Big Data, capable of leading to a paradigm shift in the analysis of information,[15] are found in not having been extrapolated from representative samples by complex procedures,[16] but from the whole population observed, so that, in exploiting any possible correlation, in terms of predictive efficacy, their quantity prevails over the accuracy of the analysis procedure.[17] In Big Data analysis, then, predictions appear more significant than the information consciously released by users[18] making the same traditional distinction between personal data and non-personal data overcome.[19] An efficient use of Big Data, using Data Mining[20] or the latest Business Analytics[21] tools both paid, through the use of a particularly high number of variables that sometimes makes it difficult even to reconstruct the logic of the decision-making process,[22] to find hidden patterns and predictive rules,[23] represents for companies a critical as an undoubted competitive advantage,[24] provoking widespread entrepreneurial

[11] M. Delmastro and A. Nicita, *Big data. Come stanno cambiando il nostro mondo* (Il Mulino 2019), 35.

[12] For a useful definition of the algorithm, its characteristics and properties, A. C. Amato Mangiameli, *Informatica Giuridica. Appunti e materiali ad uso di lezioni* (Giappichelli 2015), 132-134.

[13] Delmastro and Nicita (n 11), 25-29; For an up-to-date delineation of Big Data requirements, M. Palmirani, 'Big data e conoscenza' (2020) Rivista di filosofia del diritto 77.

[14] Delmastro and Nicita (n 11), 10.

[15] A. Simoncini and S. Suweis, 'Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale' (2019) Rivista di filosofia del diritto 92.

[16] A. C. Amato Mangiameli, 'Algoritmi e big data. Dalla carta sulla robotica' (2019) Rivista di filosofia del diritto 112.

[17] Orefice (n 8), 149 ff.

[18] Delmastro and Nicita (n 11), 36.

[19] Ibid.

[20] For a complete analysis of the problems of *Data Mining*, C. Sarra, 'Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining', in P. Moro and C. Sarra (eds), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica* (Franco Angeli 2017) 41 ff. On the use of neural networks and of supervised and unsupervised learning algorithms, Amato Mangiameli (n 16), 108; G. De Anna, 'Automi, responsabilità e diritto' (2019) Rivista di filosofia del diritto 131.

[21] *Business Analytics* can be here summarily defined as the set of tools and software applications for accessing, analyzing and viewing data that helps management quickly grasp the relevant information and control company performance in making the most effective decisions.

[22] De Tullio (n 9), 640.

[23] Ibid., 639 and 650. A possible solution, envisaged to overcome the problem, has been identified in the limitation of the maximum number of variables to be used in Big Data analysis, but the problem of unexpectedly extracted data, as well as additional data, would remain open, even in this hypothesis information obtained thanks to the predictive effectiveness of the algorithms used, F. Casi, 'Big Data ed etica dei dati' (28 December 2018) Consulta di Bioetica Onlus <https://www.consultadibioetica.org/big-data-ed-etica-dei-dati-di-fiorello-casi>.

[24] See, for example, 'Profilazione 2.0: dimmi come clicchi e ti dirò chi sei' (28 September 2010) MyMarketing.net <http://mymarketingnet.blog.kataweb.it/2010/09/28/dimmi-come-clicchi-e-ti-diro-chi-sei/>.

opposition to some policies on data portability.[25] The economic value of Big data is a product of the refinement of knowledge extraction techniques, rather than the amount of data itself.[26] The possibility of collecting, processing and crossing personal information progressively assimilates individuals to sensors in the environment[27] and leads to a redefinition of individual self-determination capable of placing knowledge and the effectiveness of its guarantee at the center of reflection.

3. *Big Data and Privacy*

A significant problem concerns the difficulty in establishing when and to what extent the user is actually aware of the collection of personal data[28] and is free to consent to their processing – considering that access to specific data is not always an indispensable condition for the use of a service, in the light of IT mechanisms, such as tracking walls, which can exclude from a particular service users who refuse to extend the consent provided to it also for another service[29] or who act as marginalizing factors and forcing consent, as happens in the case of devices tracking.[30] The doubts about the freedom in the granting of consent are further intensified if only we consider the current indispensability of some services in interpersonal communications:[31] the apparently free acceptance of users allows companies to exploit personal information, posing serious questions on the protection of confidentiality and freedom of expression, as, in order to "hide", the individual could, as a last resort, renounce the freedom to choose the contents to access and the sites to visit on the Net.[32] In this case, the refusal to provide their information "would imply exclusion from an increasing number of social processes, from access to knowledge to the supply of goods and services",[33] thereby damaging individual and community rights. The protection of privacy appears, in fact, entrusted to an unfair negotiation between entrepreneur and consumer which for the latter is resolved in a mere take or leave,[34] a

[25] Orefice (n 8), 62.

[26] G. Della Morte, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti* (Editoriale Scientifica 2019), 161.

[27] Talia (n 2), 81.

[28] Amato Mangiameli (n 16), 112.

[29] A. C. Zanuzzi, 'Internet of things e privacy. Sicurezza e autodeterminazione informativa', in P. Moro and C. Sarra (eds), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica* (Franco Angeli 2017) 115.

[30] Ibid. 116-118.

[31] Consequently, it can be understood that the information for the granting of consent, although compliant with the 2016 Regulation, does not seem sufficiently effective to stem the increasing use of Big Data in the market and their predictive potential, lending themselves to applications mostly formalistic, Delmastro and Nicita (n 11), 142.

[32] Orefice (n 8), 106-107; S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli* (Laterza, 2012) 26.

[33] Ibid. 29. These practices, although widespread, are in contrast with Art. 4 GDPR, concerning informed consent: in fact, a request that includes non-homogeneous purposes or that prevents or disturbs the use of a service offered online is not compliant with the Regulation, as well as with the requirement of the freedom of consent, given that the latter cannot be considered effectively free when its transfer constitutes the price of the service; see Orefice (n 8), 110-111.

[34] On the need to set competition policies using criteria that take privacy into due account and, more generally, on the link between privacy and competition, G. De Minico*,* 'Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria' (2019) Diritto pubblico 89, 109-113.

situation aggravated by the circumstance that frequently sees the user sign a single contract with the same supplier of services, transferring huge amounts of information into the hands of a single subject,[35] with profound repercussions on individual and collective self-determination of information.[36] In such cases, the withdrawal of consent appears to be an ineffective and hypocritical remedy since it keeps the owner of the information in a subordinate condition, being effectively excluded from an autonomous decision-making power over his own data.[37] In the Internet of Things sector, there is also a concrete risk of involuntary activation of the smart device and unconscious transfer of data, with a clear loss of information control and decision-making power on the user's personal information.[38] It is also necessary to highlight how the evaluation of the freedom and awareness of consent to processing would concern personal data, that is, referable to specific interested parties, while Big Data tends to work on anonymous data: in this regard, it does not seem to be excluded anyway a reason for damage as Big Data, while using anonymous data, after appropriate correlations,[39] become referable to very specific people.[40] In any case, the European legislative framework, while not directly contemplating Big Data,[41] establishes some fundamental principles in the collection and use of personal

[35] Palanza (n 3), 3.

[36] De Tullio (n 9), 665.

[37] Ibid.

[38] Zanuzzi (n 29), 110. It should be remembered the Opinion 8/2014 of WP29 which specifies that, in order to the processing to be considered lawful, users must remain in full control of their data throughout the life cycle of the device. The critical issues mentioned could be referred both to the nature of the device of smart objects as to a lack of coordination between the stakeholders in the processing of personal data, in relation to the adoption of the necessary minimum security measures, see id., 103-106. In the first hypothesis, one could appeal to compliance with the *privacy by design* criterion that is expressed by Art. 25 GDPR, which anticipates the protection of personal data from the planning of the treatment. It should also be mentioned Art. 32 of the Privacy Code which obligates electronic communications service providers to adopt the "technical and organizational measures appropriate to the existing risk to safeguard the security of its services and to comply with the provisions of Art. 32 bis" (i.e. for notifications in the event of data breach). In the same line of guarantee of personal information, Art. 24 GDPR indicates the *accountability* principle, referring to the set of measures that the data controller and the data processor must implement to "guarantee and be able to demonstrate that the processing is carried out in accordance with this regulation". This is a criterion suitable for investing the entirety of company operations, F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Giappichelli 2016), 288. The guarantee of privacy by design and the accountability are accompanied by the respect for *privacy by default*, Art. 25 GDPR, which provides that only the personal data necessary and sufficient for each specific processing purpose and for the period strictly necessary for these purposes are processed by default. On this argument, see Iasselli (n 4), 180-181. Finally, the mentioned criteria are flanked by Recital 78 GDPR which states that "the protection of the rights and freedoms of individuals with regard to the processing of personal data requires the adoption of adequate technical and organizational measures to guarantee compliance with the provisions of this Regulation […]. Such measures could consist, inter alia, in minimizing the processing of personal data, pseudonymising personal data as soon as possible, offering transparency regarding the functions and processing of personal data, allowing the data subject to control the data processing and allow the data controller to create and improve the security features".

[39] Della Morte (n 26), 161.

[40] De Minico (n 34), 95.

[41] It should be noted that the European Regulation does not make direct mention of Big Data, excluding from consideration data capable of returning information that is sometimes more than sensitive about the individual and capable of profoundly affecting the expression of fundamental rights.

information and, as recent judgments of the Court of Justice of the EU highlight, the need for an effective data protection which should, in principle, prevail over economic interests,[42] considering privacy as an inviolable and essential right both for the formation of the individual personality and for the development of relationships.[43] In this regard, we can only mention here an articulated and exemplary ruling of the German Federal Constitutional Court of 15 December 1983 – with which a real theory on informative self-determination is elaborated – built on the assumption that if on the one hand the individual cannot be exclusive owner of his data – which, representing the social reality, are considered as neutral information – has the right to control over the latter, representing the same a manifestation of the right to the full development of his personality, attributing to the legislator a role of balancing assumptions and contexts that make it possible to limit the right to privacy.[44] Finally, the EDPS, in various opinions and initiatives, did not fail to underline the importance of a consistent regulatory application in the era of Big Data, elaborating the concept of protection of personal information and underlining the need to seize the opportunities offered by new technologies, without allowing them to determine the social values of reference.[45] The challenge to be grasped – and for which the traditional rules and principles that can be deduced from international and national law often appear inadequate and obsolete, suggesting highly deformed systems and technical solutions delegated to private subjects[46] – is to harmonize often conflicting interests and needs, such as transparency and confidentiality of information, data protection and global security,[47] privacy and right to be informed, obtaining an adequate balance between market logic and the essential guarantee of prevailing and non-negotiable rights.[48]

4. *Big Data and Information*

The cooperative and participatory use in the public sphere of some types of Big Data can have a strong social interest, just think of the sharing of information in a smart city, of the monitoring of data aimed at implementing environmental protection and, above all, of the scientific context where the sharing of Big Data opens up to the dispensing of scientific research and its results.[49] In such cases, the information

[42] European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, P8_TA(2017)0076.

[43] De Tullio (n 9), 653.

[44] Cf. Bundesverfassungsgericht, 15.12.1983, 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83; Della Morte (n 26), 166.

[45] European Parliament, Plenary session 2/03/2017.

[46] On the dialectic and the equilibrium of the main "axes of tension" between opposing rights, Della Morte (n 26), 175-227.

[47] For Ziccardi, the debate would concern not so much security as the real possibility of global surveillance, G. Ziccardi, *Il libro digitale dei morti. Memoria, lutto, eternità e oblio nell'era dei social network* (UTET 2017), 88.

[48] Rodotà (n 6), 21 ff. On the link and balance between constitutionally protected values such as freedom of communication, information, and protection of privacy on Web, M. C. De Vivo, 'Comunicare in Internet. Con che diritto?' (2000) Informatica e Diritto 125.

[49] Palanza (n 3), 128.

appears to be declined in favor of knowledge and equality[50] as the foundation of the democratic participation it would like – as recalled by Art. 19 of the Universal Declaration of Human Rights, as well as Art. 21 of the Italian Constitution – free and legally guaranteed access to knowledge and culture.[51] The exploitation of Big Data can be functional both to the enhancement of economic freedoms and to be at the service of inviolable rights and equality.[52] A pressing unknown factor is therefore given by the progressive concentration of information in the hands of a few operators, a phenomenon that is reflected in the full implementation of the rights of freedom and in the future of democracy. The digital platforms, called Over the Top (OTT) or *digital giants*, Big Tech, represent subjects capable of developing services hierarchically above the traditional physical infrastructures of fixed and mobile telecommunications access to the Net and able to assert a intermediation between the sides of the market based on a very high intensity technological structure and based, as regards the use of data, on vertical integration models,[53] giving rise to a marked information polarization.[54] The process of information concentration therefore seems to stand against the principle of substantial equality, which is expressed by the involvement in the cognitive process formed with the contribution of everyone,[55] as well as against the protection of competition and the legal construction of a transparent data-given market[56] that the data collected by the OTTs become the exclusive domain of a few players, able to place barriers to entry to new competitors, distorting the game of competition even in the absence of abuse,[57] to the obvious detriment of the consumer.[58] The ownership of data is then imposed as an essential facility of an intangible nature, indispensable to compete on the market, resulting in the obligation to open data for the information giants,[59] shifting attention from the element of consent to the responsibility of OTTs, in order to reduce phenomena of asymmetric distribution of information resources or undue surveillance by focusing economic processes on fundamental rights.[60] "The masses of data should be at the service of individual growth, equal access for the benefit of other operators and the

[50] On the potential of Big Data in the prevention of human rights violations, L. Nosari, 'Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani' (17 April 2018) CYBERLAWS <https://www.cyberlaws.it/2018/big-data-e-diritti-umani>.

[51] J. Drexl, 'Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of post-truth politics' (2016) Max Plank Institute for Innovation and Competition Research Paper No. 16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881191>.

[52] De Tullio (n 9), 644.

[53] Delmastro and Nicita (n 11), 51-53.

[54] Ibid. 125.

[55] De Minico (n 34), 113.

[56] Delmastro and Nicita (n 11), 31. The right to the portability of personal data, structured and unstructured, enshrined in Art. 20 GDPR, seems to correspond to this logic, id. 129-130.

[57] De Tullio (n 9), 660. Art. 102 TFEU requires the abuse in addition to market power and a significant price increase, that is, it does not punish market dominance in itself but its misuse to the detriment of consumers and competitors. In any case, any sanctioning measures could not be resolved in mere repressive orders of anticompetitive conduct but should be *privacy based*. On the ways in which the classic remedies of antitrust law could operate in *data driven* digital markets; see De Minico (n 34), 103-109.

[58] Orefice (n 8), 11.

[59] Ibid., 13.

[60] Ibid.

return of data to those who procured them ab initio".[61] In a system inspired by the aims of political, economic and social solidarity, aimed at achieving the full development of the person – Art. 2 Italian Constitution – the data collected by companies should be common goods whose open access, compatibly with privacy needs, subtracts the democratic communication circuit from the self-referentiality of the market.

The ability of online platforms to influence appears equally effective in the political context as they can affect the choices of citizens, even reaching, in some cases distorting, the hierarchical organization, *ranking*, of the news in search, especially in the electoral period. The amount of information available online also corresponds to a greater amount of disinformation strategies based on fake news,[62] so the quality of information ultimately depends on the critical and discerning ability of the end user.[63] In these circumstances, the risk represented by the landowners of knowledge[64] in sending partial messages – frequently selected through the *Sentiment analysis*[65] and with the practice of *clickbaiting* – is evident and it is increate by the use of bait-titles created to attract clicks and arouse viewing of Web pages, capable of affecting the free action of the individual and of questioning the most basic democratic principles.[66] Individual profiling, determined by the application of the appropriate algorithms,[67] thus contributes to selecting crucial content for the formation of public opinion, to be reported to the individual as well as to the political agenda.[68] In the creation of a *filter bubble*, aimed at showing the user the information that the algorithm has calculated for him as potentially interesting,[69] all the asymmetry between the provider of the information service and the user is shown, aggravated by the absence of transparency of the criteria set underlying the functioning of the algorithm.[70] For these reasons, the importance of the *explainability* of the results produced by artificial intelligence

[61] De Minico (n 34), 101. Moreover, if we only consider the origin of the information obtained from Big Data, we can well understand how the claiming of exclusive positions is incompatible with the third party ownership with respect to the assets of the claimant, in our case the OTTs, where the only claims operable would seem more like those of a depositary of other people's assets; see id., 90.

[62] Talia (n 2), 13. In this regard, it should be remembered the mental shortcut of the "confirmation bias" for which, in the selection of relevant information, one generally feels more attracted to those that confirm the starting subjective convictions: this breach is inserted into the selection content operated by the algorithm to suggest what could probably arouse interest, based on preferences already expressed. This procedure, as can be seen, establishes a double information filter, determined by the joint action of the algorithmic choice and the confirmation bias, Delmastro and Nicita (n 11), 95-97.

[63] Ibid. 93. The Control Authority for Communications Guarantees has launched a monitoring table on the self-regulation put in place by search engines and social networks, anticipating the work started by the European Commission with the establishment of the *High Level Group on Fake News and Online disinformation*; see id., 135.

[64] Orefice (n 8), 158. The subjects able to carry out an effective concentration of information are represented not only by Google, Facebook or Microsoft, but also by authoritarian governments and government security agencies on anti-terrorist mission: on the numerous legislative initiatives, which multiplied mainly after 11 September 2001 and directed to counter international terrorism; see Palanza (n 3), 14.

[65] Talia (n 2), 101; Orefice (n 8), 25.

[66] Ibid. 158 and 182; Simoncini and Suweis (n 15), 94 ff.

[67] Amato Mangiameli (n 16), 109.

[68] Delmastro and Nicita (n 11), 91.

[69] Amato Mangiameli (n 16),109.

[70] Talia (n 2), 97.

algorithms should be highlighted, in addition to the *knowability* of the automated decision-making process and of the data used in it, especially when they have the task of deciding in a completely automated way, producing legal effects and significantly affecting personal rights and freedoms.[71] The algorithmic logic of the predictive type, which permeates the entire process of extraction, collection and storage of Big Data, is profoundly changing the traditional mechanisms of power by introducing new decision-makers[72] and raising new and pressing questions about possible dangers of algorithmic discrimination of social groups perceived as external to the social fabric and marginalized through self-fulfilling predictions.[73] The predictive analyzes can then have, then, detrimental effects for the subjects involved regardless of the error or inaccuracy of the algorithmic forecast.[74] The central question becomes how to reconcile the regulatory and prescriptive function of law – in particular of international law and of the multiple systems of protection of fundamental rights that are expressed in forms of protection of minorities – with the logic underlying policies based on the capillary collection of information and expression of the direction of prevailing forces.[75] The essential respect for the person, in the dual individual and collective dimensions, necessarily places Big Data in the social context, configuring its use as an asset to be evaluated in relation to the specific purposes of employment.[76] From this direction derives the indispensability of a correct balance with the opposing value of privacy by evaluating whether the means used are suitable, necessary, proportionate to its pursuit:[77] the protection of personal confidentiality appears to prevail over the identification of market models and of typical consumers, in coherent explanation of Articles 41 and 42 of the Italian Constitution aimed at promoting social utility, attributed to private economic initiative, and the social function that belongs to private property.[78] In a different way, the use of Big Data currently seems to endorse economic interests or social control of the State, phenomena that require a strengthening of the guarantees payable by the citizen as well as by the community, first of all in the performance of those automated procedures aimed at take decisions that may affect the exercise of fundamental rights. Once again, all the urgency of an effective regulation of Big Data and, more generally, of personal information circulating online is shown, inspired by constitutionally guaranteed values[79] and based on globally recognized principles of protection of privacy,[80] aimed mainly at protection of the individual from the improper use of information technologies,

[71] Palmirani (n 13), 73-92.

[72] Della Morte (n 26), 8.

[73] De Tullio (n 9), 662.

[74] De Minico (n 34), 97. In the treatment of Big Data, this would entail, according to the author, an unavoidable factor of uncertainty, a "forecast risk", falling within the more general business risk, such as to generate, for the author of the algorithm or for the its user, an increase of responsibility, having to respond in the event of a harmful forecast because it discriminates against certain social categories or because it is based on erroneous calculations, regardless of the presence of negligence or willful misconduct, see id., 93-97.

[75] Della Morte (n 26), 9.

[76] De Tullio (n 9), 642.

[77] Ibid., 646.

[78] P. Perlingeri, *Il diritto civile nella legalità costituzionale* (Edizioni Scientifiche Italiane 1991), 444-445.

[79] Simoncini and Suweis (n 15), 103.

[80] Della Morte (n 26), 126.

avoiding any possible deresponsibility attributed to the interpretative capacity of the algorithms used.[81] In perspective, and also in accordance with the provisions of Art. 21 of the Italian Constitution on the freedom of expression of thought, emerges the need to evaluate access to the Internet as a fundamental right of the person and to consider knowledge as a global public good by promoting widespread use of Big Data aimed at attacking substantial inequalities and create the conditions for an authentic self-determination avoiding, except for specific hypotheses envisaged to protect the inviolable rights of the person and the community, any possible phenomenon of information closure, capable of transforming a usable good into a limited resource.[82] This would mark an important step towards shared knowledge and a properly interactive world, inaugurating an effective model of digital citizenship and generating a new form of civil solidarity fueled by information.[83] The realization, through adequate legal guarantees, of balanced social relationships opens up a possible meeting point between productive needs and human needs, in the full respect and in the enhancement of freedom, dignity and diversity of each person, elements that pertain to the intimate constitution of contemporary democracies.[84]

[81] Rodotà (n 6), 39. In this regard, see the *Statement on Algorithmic Transparency and Accountability*, 12/01/2017, published by, the US Association of Computational Mechanics (USACM), as well as the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, P8_TA(2017)0051.

[82] Rodotà (n 6), 72.

[83] Orefice (n 8), 25. In Italy, the Legislative Decree 25 May 2016, No. 97 introduced the so-called generalized access, subject to the citizen's request, followed by any response from the state administration. This procedure, however, turns out to be distant from the Open Data policy and from the full implementation of the principle of transparency, capable of feeding a network of sharing interoperability and reuse of knowledge; see id., 46-73. On the implementation of the open paradigm in the Italian legal system, id., 29 ff. On the most relevant issues concerning Open Data and the reuse of public data, see the monographic issue D. Tiscornia (ed.), *Open Data e riuso dei dati pubblici* (2011) Informatica e Diritto.

[84] S. Rodotà, 'Privacy, libertà, dignità. Discorso conclusivo della Ventiseiesima Conferenza Internazionale sulla protezione dei dati' (2004) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293>.

PROTECTION OF PERSONAL DATA AND HUMAN RIGHTS BETWEEN THE ECHR AND THE EU LEGAL ORDER

ALFREDO TERRASI

SUMMARY: 1. Introduction. – 2. Council of Europe and Data Protection. – 2.1. Data Protection before the ECtHR – 3. Data protection in EU legal system. – 3.1. Art. 8 of the Charter of Nice before the CJEU. – 3.2. Google and Facebook saga. – 4. Conclusive remarks.

1. *Introduction*

Moving from an international law perspective, in an analysis on personal data protection across Europe the focus can be set on two different but deeply linked issues: human rights protection, on the one hand, and free circulation of such data, on the other.

One can easily see that the abovementioned issues could bring to a clash, in so far as they imply different interests at stake. In other words, dealing with data protection results in the individuation of a fair balance between free movement of data and protection of individual privacy.

As a consequence, such a balance has to be settled keeping in consideration the relationship between the right to private life and the right to data protection (if it can be drawn as autonomous) or between privacy and data protection rules.

With the present paper, in fact, I will try to enlighten the differences among privacy and data protection, having regard to the case-law of the Court of Justice of the European Union (hereafter "CJEU" or "Court of Luxembourg") and the case-law of the European Court of Human Rights (hereafter "ECtHR" or "Court of Strasbourg"), taking into account the scope of the relevant norms, within the proper reference system. Consequently, the path I will follow is twofold: the EU provisions on data protection and their implementation, on the one hand, and the Council of Europe legal context for data protection, on the other.

After a brief analysis of the two above mentioned regulatory systems and the way they are interpreted by the competent Courts, I will try to draw up some brief conclusive remarks.

2. *Council of Europe and Data Protection*

Human rights treaties, both on universal and regional level, historically do not deal with the issue of data protection as such. Nor it does the European Convention of Human Rights (hereafter "ECHR" or "Strasbourg Convention"). The main reason of this lack can be found in the time of the drafting. The concept of personal data, in fact, assumed importance when the first personal computers were built.

In other words, the central role of data protection is strictly connected to the evolution of the so-called information technology and, as a consequence, since the end of seventies the Council of Europe (hereafter "CoE") has undertaken the drafting of several instruments, binding or not, which deal with the use that public authorities can make of information pertaining to individuals.

Whilst Art. 8 ECHR, establishing the right to private and family life, makes an express reference to domicile and correspondence, nothing is provided on personal information (such a lack, as we will see afterwards, significantly influences the ECtHR case-law). In order to fill the abovementioned gap, in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention on data protection) was opened to signature.[1]

Such a Convention is the cornerstone of data protection principles across Europe. It was, in fact, used by the European Commission as a starting point for the drafting of EU norms.

It's worth noting that the Convention on data protection has been complemented in 2001 by a protocol,[2] providing for obligations regarding supervisory authorities and transborder data flows and updated, in 2018, by an amending protocol.[3] These protocols were adopted in order to give an effective regulation to personal data use, taking in account the technological innovation.

In addition to the abovementioned conventional instruments, the CoE Committee of Ministers drafted several recommendations, dealing with very specific facets of personal information protection. As regards information technology issues, such as artificial intelligence or facial recognition, the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted specific guidelines.[4] Both recommendations and guidelines can be used as an interpretation aid in the implementation of the Convention on data protection.

2.1. *Data Protection before the ECtHR*

In the present paper it will not be possible to conduct a comprehensive analysis of the ECtHR case-law on personal information and their elaboration by public authorities. Such a premise, moreover, implies a relevant limit to data protection standards, as drawn by the Strasbourg Court, if one considers that obligations stemming from Art. 8 are essentially negative and thus usually impose *non facere* duties among

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981, European Treaty Series No. 108, entered into force on 1st October 1985.

[2] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, signed in Strasbourg on 8 November 2001, European Treaty Series No. 181, entered into force on 1st July 2004.

[3] With the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 10th October 2018, European Treaty Series No. 223), not yet entered into force, the CoE has brought up to date the Convention on data protection. The substantive principles on data protection laid down in such a Convention were not repealed. On the contrary these principles are now targeted to regulate the use of personal information in the digital era, through the express recognition of a right to personal autonomy and the right to control one's personal data (see, on the point, the Explanatory Report to the Amending Protocol, para. 10).

[4] Guidelines on Artificial Intelligence and Data Protection adopted on 25 January 2019 by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD (2019)01).

Member States. As a consequence, the use of personal data that private actors can make doesn't fall within the scope of the right to private life.

The ECtHR started dealing with data protection related issues at the end of seventies. In *Klass v. Germany*,[5] the Court established a particularly narrow proportionality test for secret surveillance measures (with the exception of measures adopted to face terrorism) but did not take into proper consideration the fact that such a surveillance was directed to acquire personal information about individuals.

Similarly, in the *Malone* case,[6] the Strasbourg Court, called upon to assess the consistency of wiretapping system, used by UK telecommunication authorities, with Art. 8 ECHR, concluded for the lack of legal basis for such a measure. As a consequence, the Court did not deal with the fact that the wiretapping outcome consisted in personal information on telecommunication network users.

Judge Pettiti, with a concurring opinion, considered that by wiretapping technique, "the authorities are enabled to deduce information that is not properly meant to be within their knowledge. It is known that, as far as data banks are concerned, *the processing of neutral data may be as revealing as the processing of sensitive data*" (emphasis added). Such a statement was based on the analysis of the CoE practice on data protection, with particular regard to the abovementioned Strasbourg Convention on personal data.

With the subsequent *Leander* case,[7] the concept of personal data finally steps into the ECtHR case-law. For the first time, in fact, the Court stated that both the storing and the release of personal information amount to an interference with the right to private life of the data subject. In other words, in the Court's view the fact that public authorities collect personal information about an individual, and adopt a detrimental decision based on such information, is enough to ascertain an interference in the right guaranteed by Art. 8 ECHR. However, it remains unclear whether the mere collection of personal an information about an individual by public authorities amounts to an interference with such a provision.

Kokott and Sobotta[8] argued that the crucial point is the scope of private life. In the Authors opinion, in fact, "Strasbourg requires an additional element of privacy in order for personal information to be included in the scope of private life". Such an additional element can be found, in strict connection with the circumstances of the case, in the systematic collection and storage of personal data (as in *Rotaru* case[9]) or in the fact that criminal conviction data are aged (as in *M. M.* case[10]). In *Amann* case,[11] on the contrary, the Strasbourg judges seem to consider that the storage of personal data amounts to an interference in the right to private life regardless of the concrete use of such data, without asking for further conditions. Some years later, the Grand Chamber stated, in

[5] ECtHR, *Klass and Others v. Germany*, Application No. 5029/71, judgment of 6 September 1978.

[6] ECtHR, *Malone v. UK*, Application No. 8691/79, judgment of 2 August 1984.

[7] ECtHR, *Leander v. Sweden*, Application No. 9248/81, judgment of 26 March 1987.

[8] J. KOKOTT and C. SOBOTTA, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, p. 224.

[9] ECtHR [GC], *Rotaru v. Romania*, Application No. 28341/95, judgment of 4 May 2000.

[10] ECtHR, *M. M. v. UK*, Application No. 24029/07, judgment of 13 November 2012,

[11] ECtHR, *Amann v. Switzerland*, Application No. 27798/95, judgment of 16 February 2000.

Marper case,[12] that "in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained" (para. 67).

If the Court used the Strasbourg Convention approach, it would state that any operation on personal information by public authorities amount to an interference with Art. 8 ECHR. Notwithstanding, following the case-by-case method, the Court did not clarify which factors can lead to classify on operation on personal data by national authorities as an interference within the meaning Art. 8 ECHR.

As a consequence, it is not clear whether an individual, whose data are elaborated by a state organ, can rely on the right to private life protection or not. Nor it is possible to infer from the ECtHR case-law on data protection, if Art. 8 ECHR calls on the Member States to guarantee to data subjects the right of access, rectification or erasure of personal information, elaborated by national authorities.

One could wonder whether the gap existing among right to privacy and right to data protection can be filled up or not. As already seen, it is not a theoretical question as such. On the contrary, the effectiveness of data protection can be affected by the abovementioned gap.

In recent years, the Strasbourg Court has moved towards a more data-oriented approach. In fact, the Convention on data protection, once mentioned without practical consequences, has become an important hermeneutic instrument when personal data issues are at stake. Whilst in the already cited *Leander* case the Court made no reference to such a Convention, since the *Rotaru* case, the Court seems to take into account, at least, some of the substantive principles enshrined in Art. 4 to Art. 8 of the Convention on data protection.

One could wonder whether the Court has competence on the application of the Convention on data protection or not. Pursuant to Art. 32 ECHR, in fact, "the jurisdiction of the Court shall extend to all matters concerning the interpretation and application of the Convention and the Protocols thereto". Such a provision should lead us to the conclusion that the ECtHR is not entitled to give effect to the Convention on data protection. Notwithstanding, the ECHR, as any international agreement, falls within the scope of the Vienna Convention on the Law of Treaties. As a consequence, the Court, when asked to implement the Convention, can legitimately make an interpretation consistent with Art. 31 of the abovementioned Vienna Convention.

It is worth noting that, in accordance with the abovesaid provision, treaties can be interpreted taking into account "any relevant rules of international law applicable in the relations between the parties" (Art. 31(3)(c)). If one considers that the State parties to the ECHR are parties to the Convention on data protection as well, it is unquestionable that the Strasbourg Court can rely on the latter (just like other treaties, concluded within the CoE framework) to solve hermeneutic questions related to the former.

The Court, as already pointed out, since *Rotaru* case has made use of the Convention on data protection, in two different ways: in order to confirm a decision based on other

[12] ECtHR [GC], *S. and Marper v. UK*, Applications Nos. 30562/04 and 30566/04, judgment of 4 December 2008.

provisions, on the one hand, and in order to conduct the necessity in a democratic society test, on the other. The former is not particularly relevant, since the concrete solution is based on ECHR norms; the latter, on the contrary, shows a significant change in the Court approach to data protection.

As far as ECHR apparently does not deal with personal information elaboration by public authorities, the use of specific normative parameters is crucial. The Court, in fact, in *Marper* case, implemented the substantive principles laid down in the Strasbourg Convention, embedding them in the relevant legal standard stemming from Art. 8 ECHR. In the abovementioned case, the Court was called upon to deal with the lawfulness of the storage of biometric data of non-convicted individuals after the termination of the criminal proceedings against the plaintiffs. The UK police, indeed, retained DNA profiles and fingerprints of Mr. Marper and Mr. S, even if the proceedings against them did not bring to a criminal conviction. The plaintiffs asked the police for the erasure of such biometric data and UK authorities rejected the requests.

The Strasbourg Court, once ascertained that the measures at stake were in accordance with the law and pursued a legitimate aim, dealt with the proportionality of biometric data retention, asserting that "the domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored" (para. 103). Noteworthy, the Court recalled Art. 5 of the Convention on data protection, using the same terminology of the abovementioned provision.

Moreover, in the assessment of the proportionality of the contested measures, the Court stated that the respondent State failed to strike a fair balance between the competing public and private interests, insofar as UK police could retained biometric data for an indefinite period. In *Marper*, conclusively, the Court took a substantive principle stemming from the Convention on data protection and used it to assess the necessity in a democratic society of the contested measures.

Notwithstanding, the Court kept a privacy-oriented approach, without taking into proper account the peculiarities of data protection. In other words, the data protection substantive principles violation did not absorb the proportionality assessment but were just one element in such an assessment.

Even the subsequent case-law on personal information shows the same theoretical approach. One can wonder whether the Court considers that privacy and data protection perfectly overlap or not. The scope of the right to private life is, obviously, much wider than the scope of data protection rules. But, unfortunately, the Court seems to leave outside the scope of Art. 8 some data protection issues. As a consequence, ECHR, up to now, does not guarantee effective legal standards of data protection, at least for the misuse of personal information by private entities, such as big data, commercial companies and telecommunication societies. Moreover, even when public authorities are involved, the marge of appreciation recognized under Art. 8 ECHR is broader than the exceptions to data protection principles.

If the ECHR were not able to guarantee an effective protection of personal information, it could depend on the fact that a right to data protection has never been drawn up by the Strasbourg Court, in the framework of the right to private life. An autonomous right to data protection, on the contrary, can be derived by the EU legal system. As a consequence, it is worth verifying the effectivity of such a right, having regard, on the one hand, to the EU regulatory framework and, on the other hand, the case-law of the CJEU.

3. *Data protection in EU legal system*

European Union, since the nineties, issued a comprehensive piece of legislation on data protection and data free movement within the EU Member States (directive 95/46/CE,[13] hereafter "data protection directive"). Even if some of the substantive principles on data elaboration overlap with the corresponding principles laid down in the Convention on data protection, the rationale of the former is quite different form the rationale of the latter, insofar as the establishment of data protection rules is a prerequisite for the circulation of data across Europe.

It is worth noting that in the Charter of Fundamental Rights of the European Union (hereafter "Charter of Nice") a right to data protection has been clearly defined in Art. 8, whilst the right to private life is provided for in Art. 7. It is well known that the Charter of Nice has become a binding primary piece of legislation with the entry into force of the so-called Lisbon Treaty.

In the Praesidium explanations relating to the Charter,[14] an explicit reference was made to the data protection directive, as well as to Art. 286 of the EC Treaty (replaced by Art. 16 of Treaty on the Functioning of the European Union). Moreover, the Praesidium mentioned the Convention on data protection and Art. 8 ECHR as further basis for the drafting of Art. 8 of the Charter.

One can wonder whether such references can influence the implementation of the right to data protection in EU or not. It is, in fact, difficult to see how a EU secondary law can be used to interpret a EU primary provision.

One more element to take into account in this patchwork normative framework is, obviously, the entry into force, in 2018, of the General Regulation on Data Protection[15] (GDPR). Such an instrument, in fact, repeals the data protection directive. As a consequence, the GDPR could have an influence on the scope of Art. 8 of the Charter.

It has to be noted that Art. 8 of the Charter did not get a concrete judicial implementation before 2014, leaving unsolved several issues on the human rights standards stemming from it.

3.1. *Art. 8 of the Charter on Nice before the CJEU*

The Court of Luxembourg started dealing with data protection issues in 2003, with two decisions that shaped the scope of the data protection directive.[16] A step forward

[13] Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[14] Explanations Relating to the Charter of Fundamental Rights of the European Union, in European Union Official Journal C 303/02 of 14th December 2007, p. 320-321.

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

[16] CJEU, case C-465/00, *Österreichischer Rundfunk*, judgment of 20 May 2003, and case C-101/01, *Bodil Lindqvist*, judgment of 6 November 2003.

in drawing an autonomous right to data protection was done in 2014[17] and 2015.[18] The Court, in fact, finally relied on the Charter of Nice, in order to determine the legality of EU secondary legislation dealing with personal information elaboration.

In the first of the abovementioned decisions, the Court dealt with the consistency of the so-called data retention directive[19] with Articles 7 and 8 of the Charter. Noteworthy, the Court used the aforementioned provisions as the only relevant standard of review. More particularly, the Irish High Court delivered a request for preliminary ruling to the CJEU, in order to ascertain whether the directive at stake was legal or not. Such a piece of legislation, in fact, required the telecommunication companies and internet providers to retain a huge amount of data (as set forth in Art. 5 of the directive) concerning fixed network telephony, mobile telephony and internet access.

First of all, the Court dealt with the scope of Articles 7 and 8 if the Charter, affirming that the collection and storage of data by telephone and internet companies fell within such a scope. Whilst the relevance of the right to private life of individuals whose communication data were stored under the data retention directive was undisputed, it is worth noting that the Court conceded that both the storing of such data and the access of the competent national authorities to the data amounted to an interference in the right to data protection, as laid down in Art. 8 of the Charter.

The Luxembourg judges considered that the abovementioned interferences respected the essence[20] of the fundamental rights at stake (within the meaning of Art. 52(1) of the Charter). Such a conclusion is not convincing, at least as Art. 8 is concerned, if one considers that the directive required to communication companies to retain the data of any individual for a period between six months and two years and to transfer such data to national authorities upon request. As a matter of fact, we are dealing with a bulk storage of personal information, on the one hand, and with a violation of the purpose limitation principle, insofar as the data were collected by the companies in order to execute a contractual obligation and then transferred to national authorities for law enforcement aims, on the other.

The Court, in the end, decided to declare invalid the whole data retention directive, on the ground of the lack of proportionality (the strict necessity test) in terms of limitation of the right to data protection and the right to private life. In the Court view the directive "applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives" and "it therefore entails an interference with the fundamental rights of practically the entire European population" (para. 56).

In other words, the CJEU declared the data retention directive invalid because of the excessively wide scope and because of the absence of substantive and procedural

[17] CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, judgment of 8 April 2014, and [GC] case C-131/12, *Google Spain SL*, judgment of 13 May 2014.

[18] CJEU [GC], case C-362/14, *Maximilian Schrems*, judgment of 6 October 2015.

[19] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[20] As observed by Brkan (M. BRKAN, *The Essence of the Fundamental Right to Privacy and Data Protection: Finding the Way Through the Maze pf the CJEU's Constitutional Reasoning*, in *German Law Journal*, 2019, p. 868), the Court "acknowledges the independent value of the concept of essence by markedly verifying whether the essence of the fundamental rights has been interfered with".

conditions to file a complaint to national authorities. However, one point remains unclear: the relationship between Art. 7 and Art. 8. The legal reasoning on the point is that "the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter" (para. 53). One could wonder whether the violation of Art. 8 entails the simultaneous violation of Art. 7 or not. If so, one should reach the conclusion that the right to data protection, in the EU legal order, is a specification of the right to private life rather than an autonomous fundamental right.

3.2. *Google and Facebook saga*

After Digital Rights Ireland decision, the Court dealt with two issues that involved big data (Facebook and Google) and became a kind of saga, with decisions in 2014-15 and then in 2019-20. I will try to briefly analyse such decisions, from the point of view of the interaction between Art. 7 and Art. 8.

In *Google Spain* case, the Court undertook an analysis on browsers responsibility for the content of third parties' webpages, from a data protection perspective. Spanish judges, in fact, addressed a request for preliminary ruling, asking the Court to ascertain whether search engines, pursuant to the data protection directive, could be considered as data processors.[21]

In the Court's view, Google could be considered, under Art. 2(d) of the data protection directive, as data controller. As a consequence, it could be held responsible of data protection rules violations.

Noteworthy, the Court argued that, in order to ascertain if data processing was legitimate, Art. 7(f), of the directive had to be interpreted in the light of Articles 7 and 8 of the Charter. Significantly, the Court expressly stated that "processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name" (para. 80). Being such an interference potentially serious, the search engines rights under data protection directive should not necessarily override internet users' interest. On the contrary, such a balance has to be struck, having regard to the nature of the information in question and its sensitivity for the data subject's private life.

Conclusively the Court affirmed that the directive at stake, interpreted in the light of Articles 7 and 8 of the Charter, recognizes the prevailing interest of the data subject over the economic interest of the operator of the search engine but also over the interest of the general public in having access to that information upon a search relating to the data subject's name.

In *Google Spain* the Court used the abovementioned Charter provision as a hermeneutic canon, whilst in Digital Rights Ireland they were considered as standard

[21] On the point, the Court stated that "in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results" (para. 28). Therefore, Luxembourg judges gave a broad interpretation of data protection directive' scope.

of review. In both cases, anyway, Articles 7 and 8 have been used simultaneously, without shaping a difference between their scopes.

The Court came back to speak out on search engines obligation to anonymize search results upon request of the data subject in 2019,[22] when required by French data protection authority for a preliminary ruling. Apparently, the Court did not rely on the Charter, in order to determine the extension of the de-referencing obligation for search engine operators, when required to do so by the data subject. On the contrary, Luxembourg judges based the decision on Art. 17 GDPR (dealing with the right to be forgotten), even if request for a preliminary ruling was issued by French authorities when the data protection directive was still applicable.

Quite surprisingly, the Court stated that the de-referencing obligation stemming from Art. 17 GDPR did not compel Google to erase any reference to the data subject asking for it from all the versions of the search engines. On the contrary, such a de-referencing is compulsory only on the versions of that search engine corresponding to all the Member States. If one considers that internet users can search the internet through search engines of third countries, the statement of the CJEU creates a lack of protection insofar as the right to be forgotten (within the meaning of Art. 17 GDPR) is substantially ineffective. As a consequence, such an interpretation of the abovementioned provision does not seem to be consistent with the right to data protection, as enshrined in Art. 8, at least as regards the right to rectification (which includes the right to erasure).

Moving from Google to Facebook, it is worth noting that the Court had to deal with a very difficult issue: the rules applicable to transborder data flows across the Atlantic Ocean. In effect, the case-law on transborder data flows is very complex, as far as law enforcement and commercial issues are involved.[23] The present analysis is focused on a particular case: how can private companies transfer data, collected in the EU (and which follow under the scope of data protection directive and GDPR), to the United States.

In 2015 the Court had to deal with the consistency of Facebook automatic data transfer from EU servers to US servers with the EU legal order. The legal basis for such a transfer was the so-called safe harbour (established by a European Commission decision on adequacy[24] of the level of data protection US legal order can afford to data). Insofar as US do not have a federal legislation on data protection, the EU Commission, laying on Art. 25(6), of data protection directive, established a kind of self-regulation

[22] CJEU [GC], case C-507/17, *Google LLC*, judgment of 24 September 2019.

[23] For a comprehensive analysis of the data flow among EU and US, see W. GREGORY VOSS, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) Washington International Law Journal 485.

[24] Pursuant to Art. 25 of the data protection directive, EU Member State can authorize transborder data flows only if the recipient (third) State ensures "an adequate level of protection". Such an adequacy finding is usually made by the European Commission with a decision. With regard to the US legal order, the absence of common data protection rules within the Federation prevented the Commission from assessing the adequacy of US as such. Consequently, with decision 2000/520/EC, adopted on the basis of Art. 25(6) of the directive, the Commission established that "the Safe Harbour Privacy Principles, as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States".

code that US companies had to sign in order to legitimately receive data collected in EU.

Such a system relied on declarations made by US companies, committing to respect the safe harbour data protection principles, under the control of the US Department of Commerce. Right to privacy and right to data protection of European citizens were very ineffective, if one considers that, *inter alia*, no redress was recognized by US legal order. Consequently, the CJEU, on the basis of a request for a preliminary ruling issued by Irish High Court, had to deal with the consistency of the safe harbour system with Articles 7 and 8 of the Charter.

The Court declared the Commission decision invalid, interpreting Art. 25(6) of the data protection directive in the light of the abovementioned fundamental rights. More precisely, according to the Court the ineffective protection of data, transferred from the European Union to the United States, had to be qualified as an interference with Article 7 and 8 of the Charter and such interference could be consistent with the Charter only in so far as it was strictly necessary. Moreover, in the Court's view, "legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception" (para. 93).

In the case at stake, Articles 7 and 8 of the Charter were considered as a unique interpretative yardstick and, just as in *Digital Rights Ireland*, the Court did not shape a distinction between right to private life scope and right to data protection scope.

After the safe harbour system was declared void, European and American authorities negotiated in order to adopt a new legal basis for transborder data flows between private entities. The negotiation led to the approval of the Privacy Shield.[25] Such a data transfer mechanism, however, was brought before the CJEU, which rendered the decision so-called *Schrems II*.[26]

It is a very recent and controversial decision, insofar as the Court was asked to forbid any data flow which involved companies on the two sides of the Atlantic Ocean. Once again, Facebook data transfers from Ireland to US were at stake, after a request for preliminary ruling filed by the Irish High Court.

The main difference between *Schrems I* and *Schrems* II is that the complaint was suited to the Irish High Court when GDPR was already in force. As a consequence, the Court took into account Art. 46 GDPR instead of Art. 25 of the data protection directive. However, the Privacy Shield was approved under the latter provision and it is not clear whether the *tempus regit actum* principle was deemed relevant or not.

Moving from a human rights' perspective, the Court dealt with the circumstance that commercial data on individuals, once transferred to US companies, could be in the availability of US law enforcement surveillance programs, since companies could be asked for data without specific rules.[27] According to the CJEU, in fact, the provision of

[25] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176).

[26] CJEU [GC], case C-311/18, *Maximilian Schrems v. Facebook Ireland LTD*, judgment of 16 July 2020.

[27] The Court observed, on the point, that "It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes

the privacy shield dealing with that issue did not grant data subjects actionable rights before the courts against the US authorities.

Consequently, in the Court's view, the lack of limitations for US law enforcement authorities, when accessing personal data transferred pursuant to the Privacy Shield, was not consistent with Art. 45 GDPR, interpreted in the light of Articles 7 and 8 of the Charter, insofar as "the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights" (para. 181).

From the brief analysis of the abovementioned CJEU decisions, it might be possible to infer that in the EU legal order data protection issues are deemed crucial. GDPR rules seem to be more privacy oriented than data protection directive ones; moreover, the Court makes reference to Articles 7 and 8 of the Charter quite often, in order to interpret data elaboration criteria in the light of fundamental rights issues.

4. *Conclusive remarks*

Data protection issues are gaining great importance both from a legal and a political point of view. I have tried to shape a kind of common thread with regard to the definition of legal data protection standards in the EU and in the CoE systems.

The norms on data elaboration differ, so as their rationale, in the two abovementioned frameworks. One could think that data protection is more effective within the Council of Europe context than in the EU legal order, insofar as the the CoE main focus is on human rights, whilst EU protects the four freedom of circulation as well as human rights.

Notwithstanding, from the analysis just carried out on ECtHR and CJEU case-law on data protection emerges a quite different result. The Strasbourg Court, in fact, manages data protection issues in the light of Art. 8 ECHR and, thus, privacy related matters seem to absorb them in a proportionality exam. The ECtHR case-law, in fact, shows the lack of awareness with regard to data protection rules, even when the Court has recourse to the data substantive principles stemming from the Convention on data protection.

On the contrary, the Luxembourg Court has acquired a relevant expertise on data protection rules. Obviously, it depends on the fact that EU legal order, since the nineties, have several norms, both on primary and secondary level, dealing with personal information elaboration. Moreover, the binding nature of the Charter of Nice has brought Art. 8 to become a cornerstone of the whole data protection framework. The Court, in fact, since 2014 has issued some decisions, dealing with either interpretation or validity of secondary norms on data protection, and the right to data protection, enshrined in Art. 8 of the Charter is always a hermeneutic parameter.

However, there is one thing that brings together Luxembourg and Strasbourg in dealing with data protection: neither the former nor the latter have shaped, up to now, a coherent definition of the individual right to data protection. And none of them

of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes" (para. 180).

succeeded in, or even tried to, drawing up a distinction between right to private life scope and right to data protection scope. As a consequence, it remains unclear whether the latter can be implemented autonomously or an interference in the right to data protection always amount to an interference in the right to private life as well.

PROMOTING A COMMON UNDERSTANDING OF THE GDPR: EUROPEAN DATA PROTECTION BOARD AND NATIONAL DATA PROTECTION AUTHORITIES

MARCO MACCHIA

SUMMARY: 1. The use of personal data in the course of political campaigns. – 2. The Powers of Domestic Authorities between Advocacy and Enforcement. – 3. The allocation of Powers between National Authorities: The Decentralized Cooperation. – 4. The Consistency Mechanism. – 5. Administrative Decentralization and Vertical Independence.

1. *The use of personal data in the course of political campaigns*

A natural person – who is able to self-determine the extent to which information about him or her, including that relating to political orientation – can form own opinion more freely and consciously. The use of behavioural advertising techniques in politics, with the delivery of targeted electoral messages, risks compromising pluralism of information and the voter's ability to seek new and different information. The lack of transparency in the collection and use of these data undermines citizens' trust in the democratic system and can lead to a deep crisis of legitimacy.

Engaging with voters is inherent to the democratic process. It allows the preparation of political programmes, enables citizens to influence politics, and supports the development of campaigns in line with citizens expectations. Political parties, political coalitions and candidates increasingly rely on personal data and sophisticated profiling techniques to monitor and target voters and opinion leaders. In practice, individuals receive highly personalised messages and information, especially on social media platforms, on the basis of personal interests, lifestyle habits and values.

An infringement of the right to protection of personal data could affect fundamental rights, such as freedom of expression, freedom to hold opinions and the possibility to think liberally without manipulation. Ahead of the elections to the European Parliament and other elections in the EU scheduled for 2019, the European Data Protection Board (hereinafter EDPB) set out a catalogue of measures to be respected when political parties process personal data in the course of electoral activities.

When political parties and candidate use personal data collected through social media, they need to observe the duty to be transparent and provide sufficient information to the individuals who are being analysed and whose personal data are being processed. Personal data revealing political opinions represent a special category of data under the GDPR (General Data Protection Regulation 679/2016).[1] For those reasons "in case of targeting, adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it and how they can exercise their rights as data subjects". "Compliance with data protection

[1] See O. Lynskey, 'The "Europeanisation" of Data Protection Law' (2017) 19 Cambridge Yearbook of European Legal Studies, 259; H. Hijmans, *The European Union as Guardian of Internet Privacy* (Springer 2016) 17.

rules, including in the context of electoral activities and political campaigns, is essential to protect democracy. It is also a means to preserve the trust and confidence of citizens and the integrity of elections".[2]

EDPB members work together with data protection authorities to ensure consistent interpretation and compliance with the GDPR, with a view to safeguard trust in the security and integrity of the elections. In this respect, the European system for the processing and protection of personal data minimizes the risks related to the processing of personal data for political purposes. Social media, platforms, interest groups, data brokers, analytics companies, and networks are involved, as far as they play an important role in the election process.

Within the GDPR framework, independent data protection authorities monitor the enforcement and correct implementation of supranational rules in their respective jurisdiction (national perspective) and ensure, through mechanisms of coherence and close cooperation, uniform levels of protection in the European legal space (supranational perspective). The EU reinforces the terms for this cooperation through the creation of a new European body, the EDPB. What decision-making power is awarded to national authorities? How do they interact with the EDPB? How do decentralized forms of cooperation work at European level? Do they protect the vertical independence of the national authorities or do they lead to a centralization of decision-making powers within the European umbrella network?

2. *The Powers of Domestic Authorities between Advocacy and Enforcement*

The GDPR comprehensively sets out the tasks and powers of the national authorities, thus leaving limited margins of appreciation to the States and reducing the asymmetries between domestic powers in the European area due to the uniformity of the European system of guarantees. In each Member State, national authorities enjoy the same powers. This shows the trend towards a decentralized implementation of European law through national decision-making structures.

The similarities in powers between the national authorities enable the European legislator to allocate the enforcement of privacy rules primarily and almost exclusively under the responsibility of the national authorities. In this respect – contrary to other sectors, such as banking supervision –, there is no room for the centralization of enforcement/oversight powers at European level.

Alongside the typical enforcement powers of European rules, there is an increase in the advocacy functions of national authorities.[3] These tasks include advising national parliaments, governments and other institutions on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to data processing, monitoring developments potentially affecting the protection of personal data, promoting the knowledge of data controllers and data controllers about their obligations, encouraging the development and delivery of opinions on codes of

[2] See EDPB, Statement 2/2019 on the use of personal data in the course of political campaigns, adopted on 13 March 2019. See also L. Califano, 'Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network' (2019) 16 Federalismi.it (7 August 2019), 1-12.

[3] See A. Jòri, 'Shaping vs applying data protection law: two core functions of data protection authorities' (2015) 5 International Data Privacy Law 133; M. Szydło, 'Principles underlying independence of national data protection authorities: Commission v. Austria' (2013) 50 Common Market Law Review 1822.

conduct and approving those that provide a sufficient level of safeguards.[4] The 'proactive' role – by proposing regulatory input – of authorities vis-à-vis national governments has been accentuated.

In addition to their advocacy role, national authorities have investigative, corrective and licensing powers. They can order the data controller to provide any information necessary for the performance of its tasks and can obtain access to all personal data and information necessary for the performance of its institutional tasks it holds. They have a corrective function: they can impose the compliance of the processing with the regulatory provisions, the provisional or definitive reduction of processing, as well as the power to order the rectification, destruction of personal data or limitation of processing, withdraw certification, sanction and order the interruption of data flows. They can recognize certification bodies, endorse the issuing of certifications and the adoption of standard data protection clauses, and approve contractual clauses and administrative agreements.

From this brief description it is clear that the European system aims to shield the independence of national authorities also from supranational influences. What are the arguments for this? The first reason lies in the supervised asset: privacy is no longer protected with a view to establishing a uniform space to grant the free movement of data, but as an instrument for the protection of individuals. The second reason concerns the cross-cutting nature of data protection towards the private sector and the public sphere.[5] In this respect, it should be recalled that the first data protection legislation in the world - dating back to 1970 in the State of Hesse - was aimed directly at the public sector because of the strong opposition from private sector representatives to the drafting of legislation affecting their prerogatives.[6] The third factor is the shift in paradigm: we have moved from a consensual dimension of data processing to a system of prior assessment of the risks involved. The reduced relevance of users' self-determination strengthens the role of national authorities which are required to exercise technical oversight of the degree of risk involved in data processing.[7] This evolution is complemented by a transition from a follow-up protection regime (reparative protection) to a preventive one, based on *ex ante* assessments of the impact of data processing on the individual sphere.

3. *The allocation of Powers between National Authorities: The Decentralized Cooperation*

[4] According GDPR 2016, Art. 57.

[5] See Ph. Schütz, 'Comparing formal independence of data protection authorities in selected EU Member States' (2012) Conference Paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference <http://regulation.upf.edu> accessed 30 September 2020, who remarks "Despite the traditional checks and balances in a democratic and constitutional state, the monitoring of governmental bodies by an authority closely linked to the government is particularly new in the theoretical framework of the regulatory state and IRAs".

[6] See T. Hüttl, 'The content of "complete independence" contained in the Data Protection Directive' (2012) 2 International Data Privacy Law 137; A. Balthasar, 'Complete Independence of National Data Protection Supervisory Authorities. Second Try: Comments on the Judgment of the CJEU of 16 October 2012, C-614/10, with Due Regard to its Previous Judgment of 9 March 2010, C-518/07' (2013) 9 Utrecht Law Review 26.

[7] See A. Mantelero, 'Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework' (2017) 33 Computer Law & Security Review 586.

According to the territorial principle, each national supervisory authority is empowered to carry out the tasks assigned to it and to exercise the powers conferred on it only within its jurisdiction. However, it is not unusual for the processing of data to involve several Member States, in which case the powers are 'collaborative', involving all the relevant national authorities in the decision-making process. A general duty of cooperation is not only aimed at the exchange of information, but also at commonly attempting to achieve consensus.

When data processing is carried out in more than one country, a single point of contact must be identified to supervise the processing and management of personal data. Citizens may address their local authority in accordance with the proximity principle. In order to avoid the forum shopping characteristic of the former framework, the local authority will have to identify the leading authority, i.e. the supervisory body of the main or unique site of establishment of the data controller or the processor, or that of the territory in which the data subjects are substantially affected (given the dematerialised nature of the information and the use of ubiquitous vehicles).[8] In this sense, the area where the action is to be carried out is more important than the site of the establishment.

The leading authority may discretionary decide whether it wills to deal with the case. If it decides to do so, the supervisory authority that has informed the leading authority may submit a draft decision to the latter, which must be given the highest consideration. If not, the supervisory authority that has informed the leading authority shall deal with the case in accordance with the mutual assistance models. Under the cooperation model - termed the one stop shop mechanism - the leading authority may at any time request the assistance of the other national authorities concerned (including consultations and inspections) and conduct joint operations for the purpose of carrying out investigations or monitoring the implementation of a measure concerning a data controller or controller established in another Member State. Where there is a cross border processing of personal data, according to the one stop shop mechanism, the leading authority shall without delay communicate all relevant information to the national authorities concerned by submitting a draft decision to them. The authorities concerned may issue an opinion on the draft decision which must be duly taken into account in the final decision by the leading authority.

Cooperation does not stop at this stage. If the authorities concerned remain passive, their silence shall be deemed to be a presumption of consent. If the opposition to the draft decision is upheld, the amended draft decision must be submitted for a new opinion. If the objection is not accepted by the leading authority, the matter is subject to the consistency mechanism. The relevant supervisory authorities and the EDPB must be informed of the decision taken.

The implementation of the GDPR is decentralised to the national authorities and the pivotal point of the system is the identification of a leading authority that has the power to take a measure with effects beyond the national borders, as a decentralised authority for the implementation of EU law. The European dimension of the leading authority is also demonstrated by the fact that the latter may also exercise any additional

[8] Court of Justice of the EU (Grand Chamber), Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014.

powers provided under its national law within the territory of another State.[9] National authorities are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

The mechanism is based on the agreement of the national authorities and ensures consistency in matters only to the extent it is necessary, without affecting the independence of national supervisory authorities and should leave the responsibilities of the different actors where they belong. Therefore only cases of conflicts between national authorities are assigned to the consistency mechanism: if DPAs do not manage to come to an agreement, consistency will be triggered, so that the question of exclusivity of powers under the one-stop-shop does not raise issues any longer.[10] Some critical issues remain, especially with regard to access to justice. This issue emerges when, in the event of a complaint being lodged by the person affected by the processing with the authority of his own State, jurisdiction belongs to the courts of the State of the leading authority. The same situation can occur where complaints are submitted at the same time before courts established in several States, but the judicial remedy will in any case be the one in which the leading authority is established.

4. *The Consistency Mechanism*

Under this mechanism the decision-making process involves the EDPB: an independent European body which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the data protection supervisory authorities. The EDPB is composed of representatives of the national DPAs and the European Data Protection Supervisor (EDPS). Its main tasks include issuing opinions, guidelines, recommendations and best practices to promote a common understanding of the GDPR; advising the Commission on any issue related to the protection of personal data in the Union; contributing to the consistent application of the GDPR, in particular in cross-border data protection cases; promoting cooperation and the effective exchange of information and best practice between national supervisory authorities.

The consistency mechanism mainly fulfills the need to ensure cooperation. The aim is to provide advice so as to ensure the uniform application of European rules; issues of general application or having cross-border effects are subject to the consultative assessment of the EDPB. After being informed of the draft decision, the reasons and the views of the other authorities, the Board issues an opinion on the matter submitted

[9] See H. Hijmans, 'The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European?' (2016) 2 European Data Protection Law Review 362; P. de Hert and M. Czerniawski, 'Expanding the European data protection scope beyond territory: Art. 3 of the General Data Protection Regulation in its wider context' (2016) 6 International Data Privacy Law 230; P. Craig, 'Shared Administration and Networks: Global and EU Perspectives', in G. Anthony, J.-B. Auby, J. Morison and T. Zwart (eds), *Values in Global Administrative Law. Essays in Honour of Spyridon Flogaitis and Gerard Timsit* (Hart 2011) 81.

[10] A. Giurgiu and T. Larsen, 'Roles and Powers of National Data Protection Authorities. Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?' (2016) 2 European Data Protection Law Review 342. See also A. Giurgiu, G. Boulet and P. De Hert, 'EU's One-Stop-Shop Mechanism: Thinking Transnational' (2015) 137 Privacy Laws & Business. International Report 16.

by a majority of its members. The EDPB's opinion is not binding and does not override the DPA's choice, but it must be taken into the fullest account when taking the final decision.

Contrary to what happens in other networks (such as the banking union or the competition network) where mechanisms are in place to call upon the European authority to decide, in the area of personal data protection, the national authorities remain in charge of decision-making. However, when it is necessary to settle a conflict between DPAs, decision-making power is devolved to the EDPB according to a gradually increasing cooperation model. In this case, the decision is taken by a two-thirds majority within one month since referral to the EDPB, and it is binding for the national authorities. When an objection to the draft decision is raised and rejected, when conflicting views on the designation of the leading authority emerge, when the (mandatory) opinion of the EDPB is not required, the decision is delegated to the supranational body. This shows how the legislator's choice was to avoid undermining the vertical independence of national decision-makers.[11]

5. *Administrative Decentralisation and Vertical Independence*

The data protection network is a distinctive "brand new governance model".[12] The national supervisory authorities have vertical autonomy and independence vis-à-vis the Commission and the other European institutions. In cases of conflict, however, when the Committee uses binding powers, "the national DPAs are no longer sovereign to ensure the control of the EU rules on data protection"[13]

The choice of relying on a decentralized national enforcement, albeit in a European capacity, is demonstrated by the fact that the Consistency Mechanism is not a forum for concerted decision-making, but a place for resolving conflicts. The harmonization of discipline at European level has not been followed by the devolution of executive powers to supranational authorities. The weakness of the coordination and co-decision mechanisms highlights the cohabitation of national decentralized powers of an independent form, according to the logic of federalism of execution (or model of indirect administration), regardless of the extraterritorial effects of such decisions.

However, the national execution of European law is "*pro Union*" and not "*pro Statu*"[14] because national authorities operate in a European dimension by guaranteeing compliance with European standards of protection even beyond national borders. The

[11] The perspective adopted by the Commission in the draft was very divergent. The need to overcome fragmentation in data protection enforcement and to ensure uniformity of data protection protection had been translated into a cooperation mechanism of a binding (and not facultative) nature with a broader scope of application. See N. Marsch, 'Networks of Supervisory Bodies for Information Management in the European Administrative Union' (2014) 20 European Public Law 138.

[12] A29 WP, Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), WP 236 (2 February 2016) 2. See also E. Chiti, 'Decentralized Implementation. European Agencies', in R. Schütze and T. Tridimas (eds), *Oxford Principles of European Union Law, Volume I: The European Union Legal Order* (Oxford University Press 2018) 748.

[13] Hijmans (n 1) 325.

[14] R. Schütze, 'From Rome to Lisbon: 'Executive federalism' in the (new) European Union' (2010) 47 Common Market Law Review 1385; E. Chiti, 'Mismanagement by European Agencies: Concerns, Institutional Responses, and Lessons', in J.-B. Auby, E. Breen and Th. Perroud (eds), *Corruption and Conflicts of Interest. A Comparative Law Approach* (Elgar 2014) 253.

provision of equal instruments for monitoring and managing the processing of personal data among several authorities explains the extension of the territorial dimension of the effects of the national authorities' decisions.

Cooperation occurs in the form of a network of national authorities of a mainly horizontal nature, in which the executive power is entrusted to the leading authority whose acts assume an extraterritorial significance.[15] However, in the area of personal data, the cross-border dimension is very accentuated, not least because of the dematerialisation of the media through which information crosses national borders and personal data are transmitted across national boundaries at an ever-increasing rate. In theory, the Union is best placed to ensure effectively and consistently the same degree of protection for individuals whose personal data are transferred to third countries.[16] Nevertheless, the European dimension is left to soft law, the collaborative approach of national authorities and the good practices of focusing on the use of concerted rulings through cooperation.[17]

The adoption of a model that promotes the decentralized implementation of European law instead of a system of centralized enforcement also emerges from the type of European agency on which the system is based. In light of the functions and tasks performed, the EDPB seems to respond mostly to the agency model adopted in the first "waves" of the agencification process.[18] This refers to those agencies whose main activities include the gathering and dissemination of information, the coordination of European networks, the drafting of opinions, recommendations and guidelines to support the European institutions, which represent a typical feature of a soft regulation model.

In contrast to more recent progresses – characterised by the conferral of binding decision-making powers on the agencies –, the EDPB's main activities lie in advising the Commission, publishing guidelines, recommendations and best practices, as well as ensure conflict resolution in the case of setting up the consistency mechanism.[19] Also with regard to the powers of the European agency under review, the process of harmonizing European rules on the personal data protection system seems to be taking a "step back" from the most recent trends in the process of European administrative integration.

In conclusion, therefore, compared to the most recent developments in the process of European integration, the administrative set-up concerning the supervision of personal data seems to go against the latest trends, as far as it results in an increase of the scope of the executive powers of the national authorities and a reduction of the number of cases in which the function is centrally exercised by the EDPB.

[15] See S. Cassese, 'Le reti come figura organizzativa della collaborazione', in Id., *Lo spazio giuridico globale* (Laterza, 2003); C. Franchini, 'Le fasi e i caratteri del processo evolutivo dell'organizzazione amministrativa europea' (2017) Rivista italiana diritto pubblico comunitario 375.

[16] European Commission, COM/2018/043 final, 25 May 2018.

[17] Hijmans (n 9) 372.

[18] See E. Chiti, 'Les agences, l'administration indirecte et la coadministration', in J..B. Auby and J. Dutheil de la Rochère (eds), *Traité de droit administratif européen* (Bruylant 2014) 357.

[19] According GDPR 2016, Art. 70. See E. Chiti, 'European Agencies' Rule-Making, Powers, Procedures and Assessment' (2013) 19 European Law Journal 93.

PROTECTION AND TRADE OF NON-PERSONAL DATA

CRISTINA RENGHINI

SUMMARY: 1. Introduction. – 2. Distinguish personal and non-personal data. – 3. Free flow of non-personal data. 4. Regulation or auto-regulation of free-flow of data.

1. *Introduction*

As the well-known British newspaper, *The Economist*, wrote, "The world's most valuable resource is no longer oil, but data".[1] Within its Digital Single Market strategy, after the Regulation (EU) 2016/679 on the protection of personal data (hereinafter "GDPR"), the European Commission addressed its attention to data generated by machines or processes based on new technologies (as Industry 4.0). A new Regulation (EU) 2018/1807 on the free flow of non-personal data (hereinafter "FFD Regulation") came into force on 28 May 2019.

The aim of this new regulation is to remove existing obstacles connected to the free-flow of data and to enhance the data economy by facilitating cross-border exchange of data in the European Union.

Despite the importance associated with this legal text, there are few issues connected to it. The first issue is related to the indeterminate and dynamic nature of the concept of "non-personal data". In fact, the FFD Regulation does not define it, but it is limited to referring to all data that are non-personal according to the GDPR. Secondly, the FFD Regulation only set up some basic rules, in order to remove barriers to the free "movement" of data, limiting to rule a "negative integration" of the digital single market.

In this perspective, as a starting point, the notion of non-personal data will be examined. Secondly, the rules contained in the mentioned Regulation will be analysed. Finally, as the FFD Regulation only focuses on the removal of obstacles to the free-flow of data, we will discuss the applicable rules on non-personal data that could give rise to a new "data right".

2. *Distinguish personal and non-personal data*

According to its Art. 2(1), FFD Regulation applies "to the processing of electronic data other than personal data [...]". Besides the peculiar choice to qualify data as "electronic" without a proper definition, the concept of non-personal data has not been defined. They are only defined *a contrario* from personal data, as "data other than personal data as defined in point (1) of Art. 4 GDPR" (Art. 3(1) FFD Regulation). Hence, in order to qualify what is a non-personal data, it is important to identify what comes under personal data. According to Art. 4(1) GDPR, the definition of personal data is:

[1] *Fuel of the future* (6 May 2017) The Economist.

> "Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The four elements listed in Art. 4(1) GDPR, ("any information", "related to", "an identified or identifiable" and "natural person") were explained by the Article 29 Working Party.[2]

First of all, the Article 29 Working Party refers to "information" as a concept whose meaning is self-evident. In its opinion, the concept is suitable to embrace all kind of information, both objective and subjective.[3] Secondly, data is considered "related to" someone not only when it handles on a person, but also when it would be likely to impact on a person. Thirdly, a person is "identified or identifiable" when they can be distinguished from others. In order to verify if there is a concrete possibility of identification, one should take into account "all the means reasonably likely to be used such as singling out, either by the controller or *by another person*[4] to identify the natural person directly or indirectly".[5] Finally, Art. 4(2) GDPR addresses only natural persons, excluding from the scope of application legal persons or deceased persons.[6]

The resulting definition of personal data is broad and flexible,[7] with the consequence that a distinction between personal and non-personal data might be difficult. Interestingly, along these lines, it was discussed that, in the future, taking into account the broad interpretation of the legal definition of personal data and the amount of information gathered from "smart environments", every information might be related to a person, with the consequence that everything might be personal data.[8]

The opposite of personal data is anonymous data, which refers, firstly, to information not related to an identified or identifiable person from the beginning (i.e. data gathered by climate sensors); secondly, to personal data "rendered anonymous in such a manner that the data subject is not or no longer identifiable".[9] The anonymisation of personal data is different to pseudonymisation; while anonymous data can't be attributed to a specific person, pseudonymous data can be, using additional information. In this

[2] The Article 29 Working Party (Art. 29 WP) is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018, when it has been replaced by the European Data Protection Board (EDPB). See <https://ec.europa.eu/justice/article-29/documentation/index_en.htm>.

[3] CJEU, Case C-434/16, *Peter Nowak v Data Protection Commissioner*, Judgment of 20 December 2017, para. 36.

[4] CJEU, Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, Judgment of 19 October 2016. It was the first case where the Court explicitly indicated that it is not necessary "that all the information enabling the it is not required that all the information enabling the identification of the data subject must be in the hands of one person".

[5] Recital 26, GDPR.

[6] For a detailed analysis about the four elements of personal data, see N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) Law, Innovation, and Technology 40.

[7] P. Schwartz and D. Solove 'Reconciling Personal Information in the United States and European Union' (2014) California Law Review 877.

[8] Purtova (n. 6), 79.

[9] Recital 26, GDPR.

perspective, Recital 26 of GDPR adopts a "risk-based approach",[10] in order to determine if data is personal or not. Data is not personal when identification is not "reasonably likely" to happen, taking into account "all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". However, in Opinion 05/2014 on Anonymisation Techniques, the Article 29 Working Party seems to embrace a different approach: the anonymisation process has to achieve an "irreversible de-identification". In this respect, once obtained anonymous data, there shouldn't be any risks of identification. Moreover, the Working Party considers that "when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example, after removal or masking of identifiable data), the resulting dataset is still personal data".[11] From this standpoint, it emerges quite clearly the tension between the two interpretations of the anonymisation process and the uncertainty about the its assessment. Thus, the evaluation of whether data is properly anonymised depends on specific circumstances of each individual case, considering also the rapid progress of (re)identification technologies. Shortly, the borderline between personal and non-personal data is very unclear. Distinguishing and maintaining two separate legal regimes for personal data (GDPR) and non-personal data (FFD Regulation) might be very difficult.

Moreover, the notions of two kinds of data are dynamic: depending on the contest personal data might become anonymous (anonymisation) and anonymous data might become personal data (re-identifications). In any case, in the same dataset might co-exist both personal data and non-personal data (i.e. a company's tax records, mentioning the name and telephone number of the managing director of the company). Regarding the latter, the FFD Regulation provides that the two regimes apply to the two different types of data if they can be split. Most of the time this operation may be difficult, sometimes even impossible. In this perspective, when data are "inextricably linked", the GDPR fully applies to the whole mixed dataset, also when personal data represents only a small part. The notion of "inextricably linked" is not defined by the FFD Regulation. However, the European Commission, in a Guidance to the Regulation,[12] clarified the concept; personal data and non-personal data are "inextricably linked" not only when it is impossible to separate the two sets of data, but also when it would be "economically inefficient or not technically feasible". Neither the GDPR nor the FFD Regulation impose any duties to distinguish personal and non-personal data included in a mixed dataset, so that controllers can (and have to) ensure to the whole data set the higher level of data protection, considering also that the GDPR provides rules for the free flow of personal data. Taking into account the difficulties of distinguishing personal from non-personal data and the uncertainties connected to the anonymization process, this reasoning might apply also in case controllers aren't certain about the kind of data. In order to avoid the penalties provided in GDPR, they might

[10] M. Finck and F. Pallas, 'They who must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR' (2020) International Data Privacy Law 11, 14.

[11] See K. El Eman and C. Álvarez, 'A Critical Appraisal of the Article 19 Working Party Opinion 05/2014 on Data Anonymization Techniques' (2015) International Data Privacy Law 73.

[12] Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250 final, 29 May 2019.

prefer to apply GDPR rules to the mentioned borderline cases, leaving little ground of application of FFD Regulation.

3. *Free flow of non-personal data*

The aim of FFD Regulation is to ensure the free flow of non-personal data "within the Union". It therefore does not apply to processing operations taking place outside the EU.[13] The innovative capacity of the Regulation is well represented by the introduction of what can be considered the fifth freedom on the single market, the freedom of movement of data, complementing the four traditional ones (people, goods, services and capital). However, the mentioned legal text regulates only "negative" aspect, providing rules aimed at removing all barriers to the free movement of data other than personal data. Accordingly, the Regulation prohibits Member States to introduce undertakings to process or locate data within their territories by setting, for example, data localization requirements.

Through studies, public consultations and stakeholder discussions, the Commission has identified several restrictions to the location of data for storage or processing. Examples are: supervisory authorities advising financial service providers to store their data locally; professional secrecy rules requiring local data storage or processing or broad regulations requiring local storage of information generated by the public sector, whatever the sensitivity of the information.[14]

Data localisation requirements definition is quite broad; they may take different forms ("any obligation, prohibition, condition, limit or other requirement"), they may be set out not only in laws, but also in "regulations or administrative provisions of a Member State" or, even, "resulting from general and consistent administrative practices in a Member State and in bodies governed by public law", and it includes both direct and indirect measures that would restrict the free flow of data. The concept of "indirect measures" is not defined by the Regulation but should be determined on a case by case basis. Similarly to what happens with the traditional four freedoms, the Court of Justice of the European Union (hereinafter "CJEU") will play a fundamental role in defining which measures will be considered as hindering the free flow of data. As yet, the Commission gave some examples about what direct and indirect measures might be: on the one hand, direct data localisation requirements may consist of, for instance, specific duties to storing data in a specific location or in a duty to comply with specific national technical requirements; on the other hand, indirect data localisation requirements may consist of any measures preventing or making more difficult the processing of data in another member State.[15]

The FFD Regulation provides one exception to the free flow of data: data localisation requirements are forbidden "unless they are justified on the grounds of public security in compliance with principle of proportionality". "Public security" and "proportionality principle" are well-established concepts under the European Union

[13] Recital 15 and Art. 2 FFD Regulation.

[14] See IDC, European Data Market Study: Final Report (2016); M. Bauer, M. F. Ferracane Hosuk Lee-Makiyama and E. van der Marel , 'Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States' (ECIPE 2016) <https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/>.

[15] Communication from the Commission to the European Parliament and the Council (n. 12).

law and the CJEU's case-law. Regarding the public security exception, Recital 19 of FFD Regulation outlines that it has to be read in the light of Art. 52 TFUE and the case-law of the CJEU.[16] In addition, any data localisation requirements justified by public security reasons must be proportional to the protected interests. In other words, and in accordance with the case-law of the CJEU, the proportionality principle implies that, firstly, the measure has to be appropriate to attain the purpose and, secondly, the same measure does not go beyond what is necessary for that purpose.[17] Nevertheless, the prohibition of data localisation requirements is without prejudice to already existing restrictions set up by EU law.[18]

At the same time, the FFD Regulation does not affect the principle of data availability for regulatory control, as it explicitly provides that "access to data by competent authorities may not be refused on the basis that the data are processed in another Member State".[19] In this perspective, such access will have to be allowed in cases where a national authority is legally entitled to request it from a particular holder of the data, and where it is necessary for the performance of official duties of that authority. If the authority does not obtain access and no cooperation mechanism to ask for assistance from another Member State applies or exists, the FFD Regulation provides a default cooperation mechanism between competent authorities.[20] The Regulation also sets up a "single point of contact per Member State to coordinate with other Member States" and the Commission, in order to ensure the effective application of these new rules on the free flow of non-personal data.[21]

The last important cornerstone of FFD Regulation is represented by the encouragement to the "development of self-regulatory codes of conduct at Union level", in order to outline guidelines on best practices in facilitating the switching of providers, in contrast to the so-called vendor lock-in practices, and to ensure that they provide professional users with sufficiently detailed, clear and transparent information before a contract for data storage and processing is concluded.[22] Art. 6 FFD seems to create a new right of data portability for the business-to-business sector, similar to the right of portability set up by Art. 20 of the GDPR, which establish the right to transfer personal data from a controller to another. However, as mentioned before, the majority of dataset are composed by personal and non-personal data. Considering the uncertainty that surrounds the concept of non-personal data, it is important that the exercise of the right set up by Art. 6 of FFD Regulation doesn't affect the rights to data protection of any data subject involved. In this perspective, the EDPS raised this concern, demanding

[16] The leading case for the interpretation of the public security justification is CJEU, Case-72/83, *Campus Oil Limited and others v Minister for Industry and Energy and others*, Judgment of 10 July 1984. See also, for example, CJEU (Grand Chamber), Case C-145/09, *Land Baden-Württemberg v Panagiotis Tsakouridis*, Judgment of 23 November 2010 and Case C-544/15, *Sahar Fahimian v Bundesrepublik Deutschland*, Judgment of 4 April 2017.

[17] See, for example, CJEU, Case C-343/09, *Afton Chemical Limited* v *Secretary of State for Transport*, Judgment of 8 July 2010.

[18] The Guidance on FFD Regulation mentions Art. 245(2) of the Directive 2006/112/EC on the common system of value added tax, which provides that "the Member States may require taxable persons established in their territory to notify them of the place of storage, if it is outside their territory".

[19] Art. 5(1) FFD Regulation.

[20] Art. 5(2) FFD Regulation.

[21] See Art. 7 FFD Regulation.

[22] Art. 6 FFD Regulation.

that any future self-regulatory codes of conduct on porting of data facilitating the switching of providers for professional users "must be designed and drafted in such a way that the right to personal data portability provided by Article 20 of the GDPR is not undermined".[23]

4. *Regulation or auto-regulation of free-flow of data*

As mentioned before, the new FFD Regulation aims to create a free space in which the free movement of non-personal data is guaranteed. In achieving this purpose, restrictions to circulation of data are forbidden. Besides that, the Regulation does not lay down a set of rules that could harmonise or create a "new European right of non-personal data". However, the issue of the legal protection and trade of data, in particular of machine generated data, has been the core of recent debates.[24]

Existing law does not provide specific rights to data *per se*. Depending on its nature and kind, different forms of protections may apply. In this regard, it is appropriate to mention intellectual property rights, the database protection (Directive 96/9/CE) and the trade secret rules (Directive 2016/943). However, these forms of protections are not suitable to protect data as such, as they apply to only a minimum part of data.

In short, patent and copyright law do not protect information, but innovation and original works implying a creative effort.

The database directive aims to protect data with feature of originating from a protected database. According to Art. 7(1) of the database Directive, the object of this *sui generis* protection is strictly connected to "a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part" of the database. In this perspective, the CJEU emphasised the difference between generation and collection of data, excluding investments on generation of data from this *sui generis* protection.[25] This excludes data measured by sensors or machine-produced in the first phase of their existence.

Regarding the trade secrets protection, it may include data as such, but the protection is based on the secrecy of the information. In fact, according to Art. 2 of Directive, a trade secret is an information which is secret, has a commercial value

[23] G. Buttarelli, 'Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free-Flow of Non-Personal Data in the European Union' (2018) EDPS <https://edps.europa.eu/sites/edp/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_en.pdf>, 5-6.

[24] See, among others, A. De Franceschi and M. Lehmann, 'Data As Tradable Commodity and New Measures for Their Protection' (2015) The Italian Law Journal, 51; H. Zech, 'Information as Property' (2015) Journal of Intellectual Property, Information Technology and E-Commerce Law 192; J. Drexl, 'Design Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) Journal of Intellectual Property, Information Technology and E-Commerce Law 257; J. Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy', in A. De Franceschi and R. Schulze (eds.), *Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice* (Beck 2019).

[25] CJEU (Grand Chamber), Case C-46/02, *Fixtures Marketing Ltd v Oy Veikkaus Ab.*, Judgment of 9 November 2004; (Grand Chamber), Case C-203/02, *The British Horseracing Board and Others*, Judgment of 9 November 2004; (Grand Chamber), Case C-338/02, *Fixtures Marketing Ltd v. Svenska Spel AB*, Judgment of 9 November 2004; (Grand Chamber), Case C-444/02, *Fixtures Marketing Ltd v. Organismos prognostikon agonon podosfairou AE (OPAP)*, Judgment of 9 November 2004.

because it is secret and "has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret". These rules are set out in order to protect valuable information from unlawful acquisition, use and disclosure. Once secrecy is lost, legal protection is lost as well.

The lack of property rights of any kinds of data brought a discussion about the introduction of a new property right on data.[26] However, creating a property right on data as such could face several problems. In a nutshell, in data processing, more than one stakeholder is involved, each one with a specific function connected to data: the data producer (who produces data through, i.e., Industry 4.0, internet of things, websites); the internet service provider (who makes possible the sharing of data); the data provider (who collects data from different sources); the data aggregator (who prepares databases for the data processing); the data analytics service provider (who provides specific software for data analysis).[27] All of them may have interest on data. Hence, the main issue is related to how to determine who is the "owner" of data. Moreover, in the legal debate, it was stressed that data is multidimensional, which includes syntactic, semantic and storage levels.[28] It is extremely difficult to specify a concept of data in order to recognise and define borders of the eventual new protection for data. Furthermore, it should be taken into account that the value of data increases when data joins an environment where information is shared and connected. Thus, any exclusive right could even represent an obstacle to the digital single market.

In sum, existing law is not optimal for data-flow and the creation of new exclusive rights on data is too complex. In such a scenario, players in the digital economy seem to be triggered to negotiate and rule the access and trade of data through contracts. Moreover, companies having access to a huge amount of data could easily incur in situations of market asymmetry, which may result in different forms of market distortion. In this regard, the unfair competition rules come into play.

In conclusion, the FFD Regulation represents only a starting point to allow and enhance the free flow of data. The "knocking down" of obstacles to the free-flow of non-personal data is just one side of the coin; in order to guarantee this new fifth freedom, the new challenge for the legislator will be to create a new legal framework which can build trust and access to data. Considering the peculiarities of data, the best solution seems to be to avoid an ownership model and to review the competition policy in order to both promote and protect the free flow of data. In particular, one initiative to take into consideration is the creation "default contract rules" in order to introduce

[26] Among others, A. Wiebe, 'Protection of industrial data – a new property right for digital economy?' (2017) Journal of Intellectual Property, Information Technology and E-Commerce Law 62; J. Drexl, 'Design Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) Journal of Intellectual Property, Information Technology and E-Commerce Law 257; L. Determann, 'No One Owns Data' (2018) Hastings Law Journal 1. For an economic analysis, W. Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (2016) Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil 989.

[27] A. Galiano, A. Leogrande, S. F. Massari and A. Massaro, 'I dati non personali: la natura e il valore' Rivista di diritto informatico 61, 71.

[28] H. Zech, 'Data as a tradeable commodity', in A. De Franceschi (ed.) *European Contract Law and the Digital Single Market* (Intersentia 2016).

an unfairness control also in Business to Business contractual relationships.[29] In this respect, it is interesting to notice that some Member State have extended the application of some Business to Consumer rules (for example the Directive 93/13/EEC on unfair terms in consumer contracts) to Business to Business models. Furthermore, it may be established a "public interest" right to data access or a licensing regime. About the latter, it may be laid down on the basis of FRAND terms (fair, reasonable and non-discriminatory) model already well-known in licensing of essential patents context.

[29] About personal data see the European Parlament and Council Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods. In this regard, see e.g. A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Edizioni scientifiche Italiane 2017).

Protection of Personal and Non-Personal Data: A Chinese Perspective

YUTING YAN

SUMMARY: 1. Introduction. – 2. Differential Protection of Data. – 2.1. The Concept of Protection of Personal Data. – 2.1.1. The Evolution of Legal Terminology. – 2.1.2. The Change of the Way of Protection. – 2.1.3. The Concept and Protection of Non-Personal Data. – 3. China's Data Protection Mechanism. – 3.1. China's Data Protection Legislation and Policy System. – 3.1.1. The Value Orientation of Equal Emphasis on Security and Development. – 3.1.2 Personal Data Protection Mechanism. – 3.1.2.1 Cross-Border Data Movements Management of Personal Data. – 3.1.2.2. Personal Data Protection for Children. – 3.1.3. Important and Sensitive Data Management System. – 3.2. Cybersecurity Law. – 3.3. Data Security Law (Draft). – 3.4. Personal Information Protection Law. – 4. Current Situation, Principles and Trends of Data Protection in China. – 4.1. Characteristics of Data Protection System. – 4.1.1. Status of Data Protection at The National Level. – 4.1.2. Status of Data Protection at the Enterprise Level. – 4.2. Problems Faced by China's Data Protection Mechanism. – 4.2.1. Lack of Comprehensive Legislative System for Data Differentiated Protection. – 4.2.2. "Data Localization" Preference Constrains China's Participation in Global Data Alliances. – 4.3. Trends: From Data Regulation to Data Governance. – 5. Building a Data differentiated Protection System in China. – 5.1. Principles. – 5.2. Domestic. – 5.2.1. Building A Multi-Subjects Data Governance System for Chinese Data. – 5.2.2. Building a State-Led Security Guarantee System for Cross-Border Data Movements. – 5.3. International.

1. *Introduction*

With the rapid development of network technology, big data technology and artificial intelligence technology, mankind has stepped into the era of digital economy, launching a new information revolution. With the deep integration of digital technology with social production and personal life, the widespread use of digital technology has become an indispensable part of people's lives and development, and the influence of data has become increasingly prominent in the public and private spheres.

The trends of integration, digitization and intellectualization for the smart society pose challenges to traditional human rights. As the digital divide widens, the issue of data movement is closely linked to national development, sovereignty, and security. The tremendous advances and gains brought about by the rapid development of information technology have become the latest field for games between individuals, society, government, and state.

The erosion towards privacy boundaries and automatic discrimination by big data technology has raised concerns about the safeguard of human rights of vulnerable groups. The rapid development of smart society and the smart world has challenged the existing logic of human rights protection. As one of the leading countries in terms of data technology and data volume, China is accelerating the establishment of data governance and safeguard system based on its national conditions.

2. *Differentiated Protection of Data*

Chinese scholars have come to believe that the trend towards differentiated protection of data is irreversible.[1]

The traditional theory that protects the data indistinguishably cannot comprehensively manage and protect data, so there is a theory tendency to distinguish between information and data,[2] between types of data[3] and types of data rights.[4] In the context of resourceful utilization of data, the only way to achieve a balance between the protection and effective use of data is to protect data differentially according to the interests represented by different types of data. differentiated protection of data refers to defining the boundaries between various data, classifying data according to their attributes, their categories, and the impact on the original data owners, etc., thereby defining the level of protection and finding a balance between data protection and utilization.

Data can be divided into personal data and non-personal data which includes enterprise data and government data, according to the different original generators or final rights attribution.[5] The key to distinguishing between personal and non-personal data is whether a specific person can be identified directly or indirectly by that data. Personal data and non-personal data are subject to different regulatory mechanisms based on different legal interests. The main conflict in the field of data protection in China currently focuses on the balance between the protection of personal rights and interests embodied in data and the economic value of data as a resource.

In terms of differentiated protection of data in law, there is no systematic and clear classification standards of data or corresponding specific provisions in current Chinese laws and regulations yet. Only the personal data has been defined by different institutions and scattered in various regulatory documents. Personal data is closely related to specific individuals, and it is mainly protected under the strict scope of personality rights in China. Conversely, personality rights no longer exist in non-personal data, which includes derivative data based on personal data, value-added data and data that exist at the stage of technological exploitation, etc. This type of data concerns the rights and obligations of enterprises with respect to their data collected and processed activities, while the government focuses on promoting the effective use and free and safe movement of non-personal data.

2.1. *The Concept and Protection of Personal Data*

[1] Li Aijun, 'Data: Its Rights Attribute and Legal Nature' (2018) 3 OL 64; Ye Ming and Wang Yan, 'Research on the Legal System of Data Island Breaking in the Age of Artificial Intelligence' (2019) 5 Journal of Dalian University of Technology(Social Sciences) 69; Liu Xinyu, 'Analysis of the Properties of Data Rights Along with System Building in the Era of Big Data' (2019) 6 Journal of Shanghai University (Social Sciences Edition) 13; Chen Bing and Gu Dandan, 'Rethinking and Restructuring of the Rational Way of Data Sharing in Digital Economy: From the Perspective of Data Typing' (2020) 4 Journal of Shanghai University of Finance and Economics 122.

[2] Zhou Sijia, 'Clarification of The Relationship Between the Right to Personal Data and the Right to Personal Information' (2020) 2 Journal of the East China University of Politics and Law 88.

[3] Liao Wensheng, 'The Protection Principle of Personal Information Data in The Era of Digital Human Rights' (2020) 4 The Northern Forum 77.

[4] Long Weiqiu, 'On the Construction of New Data Property and its System Structure' (2017) 4 Tribune of Political Science and Law 63.

[5] Xiang Dingyi and Bi Ying, 'Research on typed protection of data in big data age' (2020) 6 Journal of Chongqing University of Technology (Social Science) 94.

Chinese scholars generally identify personal data as data that, alone or in combination with other data, can identify a specific natural person.[6] In China, the concept of personal data has undergone a transformation from "personal information" to "personal data", which is mainly reflected in two aspects: the evolution of legal terminology and the change of the ways of protection.

2.1.1. *The Evolution of Legal Terminology*

The legal terminology of "personal data" in Chinese law has experienced the evolving process from "personal dignity", "personal privacy" to "personal information", until finally the legal provisions directly take "data" as the object of protection.

In 1982, Art. 38 of the Constitution of the People's Republic of China (hereinafter "Constitution")[7] states that the personal dignity of citizens of the People's Republic of China shall not be violated, which is the most fundamental legal basis for the protection of personal data.

In 1996, in the Law of the People's Republic of China on Administrative Penalty,[8] personal privacy appeared in the form of legal provisions for the first time. Then in 1998, documents indicated that personal privacy was initially protected in the form of the right to reputation.[9] The legal protection of personal privacy is widely found in various fields and departmental laws in China, such as Art. 5 of the Administrative Reconsideration Law,[10] Art. 32 of the Insurance Law,[11] Art. 39 of the Law on the Protection of Minors,[12] Articles 66 and 120 of the Civil Procedure Law,[13] and so on.

The first time "personal information" appeared in the legal provisions was in Articles 12 and 20 of the Passport Law[14] in 2007. In 2009, the terms "personal information" and "personal privacy" have become more common in laws and regulations. The recently promulgated Cybersecurity Law[15] provides a more clear and complete definition of "personal information": it "means all kinds of information recorded in an electronic or

[6] Guo Chengzhi, 'Review and Assumption of China's Personal Data Protection Framework' (2020) 2 Journal of Tianjin Sino-German University of Applied Sciences 119.

[7] Constitution of the People's Republic of China (2018 Amendment) <http://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html>.

[8] Law of the People's Republic of China on Administrative Penalty (2017 Amendment) <http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/11/content_1383613.htm>.

[9] Notice of the Supreme People's Court on Issuing the Opinions on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation) [Partially Invalid] (2017 Amendment) <http://www.lawinfochina.com/display.aspx?id=3700&lib=law>.

[10] Administrative Reconsideration Law of the People's Republic of China (2017 Amendment) <http://www.lawinfochina.com/display.aspx?id=23927&lib=law>.

[11] Insurance Law of the People's Republic of China (2015 Amendment) <http://www.lawinfochina.com/display.aspx?id=19801&lib=law>.

[12] Law of the People's Republic of China on the Protection of Minors (2012 Amendment) <http://www.lawinfochina.com/display.aspx?id=12626&lib=law>.

[13] The Civil Procedure Law of the People's Republic of China (2017 Amendment) <http://www.lawinfochina.com/display.aspx?id=23601&lib=law>.

[14] Passport Law of the People's Republic of China (2006) <http://www.lawinfochina.com/display.aspx?id=5143&lib=law>.

[15] Cybersecurity Law of the People's Republic of China (2016) <http://www.lawinfochina.com/display.aspx?id=22826&lib=law>.

other forms, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including but not limited to the natural person’s name, date of birth, identity certificate number, biology-identified personal information, address and telephone number”. It is obvious that it was greatly influenced by GDPR. The Personal Information Protection Law and the Data Security Law, which have been included in the national people's congress’s legislative plan, indicates that China has begun to explore the direct protection of data as a legal object.

2.1.2. *The Change of the Way of Protection*

Changes in China's legal provisions on personal data protection show a distinct path. Prior to 2007, the legal provisions protected personal information in general and passive ways such as privacy protection and obligations of maintaining confidentiality. After 2007, China has entered a new phase in the protection of personal information, explicitly using the term “personal information” in legal provisions, shifting from passive protection to active protection, and strengthening personal data protection through dispersed legislation[16] and amendments to existing laws and regulations.[17] Special legislation has been enacted in some industries that are particularly prone to personal data infringement, including tourism, medical care, etc. There is also corresponding legislation in the field of public administration. In 2015, China has enacted the Cybersecurity Law, which is a separate piece of legislation for the Internet that contains provisions on the definition, collection, storage, and utilization of personal data. At this stage, the path of institutional change in China’s personal data protection law is following a dispersed model of legislation. In a word, the protection of personal data for the Internet focuses on Internet security rather than providing comprehensive protection for data subjects.

From the above, personal data rights originate from the right to privacy. The separation of personal data rights and privacy rights is driven by the demand for digital life in the era of big data. With the collection, storage, transmission, processing and application of digital information, the content, values and protection mechanism of rights in the mode of privacy are facing great challenges. Extension of privacy concept to cover the flexibility of personal data, is unable to avoid large-scale personal data processing control and security risks existed in the process of data, nor to establish within the framework of traditional personality right that can weigh the personal rights protection and the development of the emerging technology industry with a relatively flexible mechanism, but it causes the mix and confusion of the traditional personality right system. Based on the above considerations, In China, the development of a new set of data rights, distinct from personality rights, began to be explored and recognized through the Personal Information Protection Law in separate legislation on personal data protection.

[16] E.g., Law of the People's Republic of China on the Protection of Minors (2012 Amendment) (n 12); Administrative License Law of the People's Republic of China (2019 Amendment) <http://www.gov.cn/flfg/2005-06/27/content_9899.htm>.

[17] E.g., Law of the People's Republic of China on Resident Identity Cards (2011 Amendment) <http://www.gov.cn/flfg/2005-06/27/content_9920.htm>; Passport Law of the People's Republic of China (2007) (n 14).

2.1.3. *The Concept and Protection of Non-Personal Data*

Non-personal data includes enterprise data as well as government data (also known as public data).

Enterprise data includes both enterprise profile data, such as enterprise name and business scope, as well as data collected or generated by the enterprise in the course of business.[18] Chinese scholars and judicial precedents tend to recognize the property rights and interests of enterprises in the competition law with respect to the data obtained by data processing activities.[19] Chinese typical cases have attempted to regulate unauthorized data crawling activities according to Anti-Unfair Competition Law and Criminal Law (e.g., the Crime of Illegally Obtaining Data from Computer System).[20]

Government data is data produced or acquired by government agencies in the course of performing their duties in accordance with the law, and recorded or preserved in a certain form, and the subject of such data is the public authority. At present, public law is mainly applicable to the protection of government data in China. China has endeavored to move towards the goal of "protecting individual privacy and safeguarding to ensure reasonable and free movements of data" in formulating rules on cross-border data movements.

In China, non-personal data is often associated with important and sensitive data, making it the object of a regime for managing cross-border data movements. In Chinese current law, important and sensitive data are subject to a regulation model with general prohibition and a graded and classified review for data cross-border movement.

3. *China's Data Protection Mechanism*

In general, China is actively developing data protection mechanisms in recent years, following the value-oriented approach of placing equal emphasis on security and development, balancing human rights protection and effective use of data, and promoting data development and sharing.

3.1. *China's Data Protection Legislation and Policy System*

The path of institutional change in China's personal data protection law is proceeding along with a dispersed legislative model. In other words, rather than unified data protection law, China currently prefers introducing data protection laws or regulations applicable to different industries based on the specific conditions of different industries and different types of specific data objects. While accelerating the development of data protection-specific legislation, the protection of personal data and the management of important and sensitive data are being strengthened through dispersed legislation and the revision of existing laws and regulations. From 2017 to 2019, China's legislative activities in the field of data protection, whether the

[18] Xu Wei, 'Reflections on the "Triple Authorization Principle" of Enterprise Data Acquisition and Its Typological" Construction' (2019) 4 SJTU Law Review 20.

[19] Li Xiaoyu, 'On the Typed Protection of Data Rights and Interests from the Perspective of Differentiating Rights' (2019) 3 Intellectual Property 50.

[20] *Sina Weibo v Pulse* (2016), Beijing Intellectual Property Court (2016) Beijing 73 Civil Judgment No. 588; *Dianping v Baidu* (2016), Shanghai Intellectual Property Court (2016) Hu 73 Civil Judgment No. 242.

development of laws and regulations or the revision of national standards, are in full swing. The Cybersecurity Law,[21] which came into effect in 2017, the Data Security Law (Draft)[22] released in 2020 and the Personal Information Protection Law,[23] which has been included in the legislative plan, are representative of China's specific legislation on data protection.

3.1.1. *The Value Orientation of Equal Emphasis on Security and Development*

China's Constitution has always maintained its position of encouraging technological innovation. In addition the Decision of the Communist Party of China (hereinafter "CPC") Central Committee on Several Major Issues Concerning Upholding and Improving the Socialist System with Chinese Characteristics and Advancing the Modernization of the National Governance System and Governance Capability[24] specified promoting the construction of digital government, strengthening orderly data sharing and protecting personal information in accordance with the law, which clarifies that the CPC Central Committee has accurately grasped the awareness and perception of the relationship between data sharing and data protection. It is important to achieve orderly data sharing while protecting personal data in accordance with the law. The State Council issued the Notice on Issuing the Action Outline for Promoting the Development of Big Data in August 2015,[25] which calls for accelerating the deployment of big data, and deepening the application of big data to ensure steady growth, promote reform, adjust structure, improve people's livelihood, and promote the modernization of governance. The Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People's Republic of China[26] issued in 2016, Chapter 27 devoted a special chapter to address "Implement the National Big Data Strategy", referring the big data as a "fundamental strategic resource". While emphasizing the acceleration of data sharing and the development of the data industry, it also pointed out the need to achieve "better protection of data resources" to safeguard the "security, effectiveness and reliability of data use". It reflects the governance principle that places equal emphasis on data security and development.

3.1.2. *Personal Data Protection Mechanism*

The landmark event in the development of data rights was the Decision of the Standing Committee of the National People's Congress on Strengthening Information

[21] Cybersecurity Law of the People's Republic of China (n 15).

[22] Data Security Law (Draft) (2019) <http://www.gov.cn/xinwen/2019-05/28/content_5395524.htm>.

[23] 'NPC Standing Committee's Legislative Affairs Commission: Personal Information Protection Law is Being Drafted' (14 May 2020) Xinhua News Agency <http://www.gov.cn/xinwen/2020-05/14/content_5511677.htm>.

[24] 'The Decision of the Communist Party of China Central Committee on Several Major Issues Concerning Upholding and Improving the Socialist System with Chinese Characteristics and Advancing the Modernization of the National Governance System and Governance Capability' (5 November 2019) Xinhua News Agency <http://www.gov.cn/zhengce/2019-11/05/content_5449023.htm>.

[25] Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data (2015) <http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm>.

[26] 'Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People's Republic of China' (17 March 2016) Xinhua News Agency <http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm>.

Protection on Networks[27] (hereinafter “Decision”) adopted by the Standing Committee of the National People's Congress (NPC) in 2012. The Decision clearly sets out the basic principles for the collection and use of personal data, especially the principles of openness and informed consent, which are closely related to personal data rights.

China’s personal data protection legislation characterized by dispersed legislation currently. Under the Constitution, branch laws,[28] judicial interpretations,[29] and national standards, various provinces and industries formulating specific rules and regulations to implement the above-mentioned data protection laws (see Table 1). At present, China is actively building a set of personal information data regulation system based on the standard of “identifiability”, covering civil law, criminal law, and administrative law. Documents above have established the principle that the right to privacy is protected and that public authority related must be exercised in accordance with the law. In recent years, the focus of legislation on personal data protection has begun to shift to the special and separate law. China is exploring formulating special laws for data protection to harmonize with existing legislation. The NPC has incorporated Data Security Law and Personal Information Protection Law in its legislative plan for the current session, and the relevant departments are working hard to study and draft them, which means that the problem of coordinating and integrating the above two sets of public law rules, the Personal Information Protection Law and the Data Security Law, with existing legislation is about to solve.

In the field of law enforcement, various departments have carried out large scale of actions to regulate the illegal collection and use of personal information in the field of apps and the Internet. In 2019, the National Information Security Standardization Technical Committee for (hereinafter “NISSTC”) released the "Information Security Technology Personal Information Security Specification (Exposure Draft). It fills in the gaps in the practical standards for personal information protection in China and has played a positive role in guiding enterprises to comply with personal data(information) protection regulations over the next year.

No.	Name	Nature	Institution	Date of issue
1	Civil Code	Law	National People's Congress	2019.12
2	Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal	Judicial Interpretation	Supreme People's Court, Supreme People's Procuratorate	2019.10

[27] ‘Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks’ (28 December 2013) Xinhua News Agency <http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm>.

[28] Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013) <http://www.gov.cn/gzdt/2013-07/19/content_2451360.htm>.

[29] Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013) <http://rmfyb.chinacourt.org/paper/images/2017-05/10/03/2017051003_pdf.pdf>.

	Activities in Relation to Information Network			
3	Measures for the Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft)	Departmental rules	Cyberspace Administration of China	2019.6
4	Provisions on the Cyber Protection of Children's Personal Information	Departmental rules	Cyberspace Administration of China	2019.8
5	Internet Personal Information Security Protection Guide	Normative Documents	Ministry of Public Security	2019.4
6	Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations	Department Working Document	Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security State, Administration for Market Regulation	2019.11
7	Information Security Technology: Personal Information Security Engineering Guide	National Standard	NISSTC	2019.5
8	Information Security Technology: Norms for the Security of Personal Information (Exposure Draft)	National Standard	NISSTC	2019.10
9	Information Security Technology: Basic Norms for the Collection of Personal Information by Mobile Internet Applications (Draft)	National Standard	NISSTC	2019.10

Tab. 1: Personal information protection normative documents in 2019

3.1.2.1. *Cross-Border Data Movements Management of Personal Data*

With respect to the cross-border movements of personal data, in 2019 the Cyberspace Administration of China (CAC) issued the Measures for the Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft)[30] and the Measures for the Administration of Data Security (Consultation Paper)[31] provided more comprehensive provisions on the protection and management of important data and personal information protection in the form of departmental rules for the first time. The documents above indicate that personal data(information) and important data will be governed differentially in terms of data cross-border security assessment.

The documents focus on the business model of network operators and recipients before personal information cross the border, whether it is legal and proper for network

[30] Measures for the Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft) (2019) <http://www.gov.cn/xinwen/2019-06/13/content_5399812.htm>.

[31] Measures for the Administration of Data Security (Consultation Paper) (2019) <http://www.gov.cn/xinwen/2019-05/28/content_5395524.htm>.

operators to obtain personal information, and whether the data transfer contract can be effectively enforced. And they clearly stipulate network operators' data protection obligations, leading network operators to proactively supervise the safety management level of overseas data recipients and providing a practical and feasible remedy for personal data subjects to protect their data rights. The emphasis on advance security assessment, supplemented by the guarantee of contractual binding, the documents reflect the management philosophy of the authorities in conducting comprehensive risk control with regard to the personal data cross-border movement.

Overall, in order to promote the free and orderly movement of personal data in accordance with the law, the documents establish an "exit before security assessment" regulatory framework based on the Cybersecurity Law and details rules on personnel structure, incidental risk control and security measures, and builds a framework for data security governance.

These provisions reflect the fact that the documents and even the future Data Security Law have broken through the traditional data security requirements of "confidentiality, integrity and availability" and extended the supervision to the data misuse activities in the process of data utilization, in order to maintain social stability and the effective use of data resources.

3.1.2.2. *Personal Data Protection for Children*

On August 23, 2019, the CAC issued the Provisions on the Cyber Protection of Children's Personal Information (hereinafter as "Child Protection Provisions").[32] The Child Protection Provisions systematically sets out the legal requirements for the protection of children's personal information and provides more specific and stricter compliance requirements for children as a special subject based on the Cybersecurity Law and other laws and regulations. The application scope of the Child Protection Provisions is relatively broad. According to Articles 2 and 3, the Regulations protect the personal information(data) of minors under the age of 14 and can apply to "collection, storage, use, transfer and disclosure of personal information from and about children through the Internet". From the text itself, any enterprise whose business involves the above-mentioned activities will likely be subject to the Child Protection Provisions.

3.1.3. *Important and Sensitive Data Management System*

In recent years, in order to be in line with the international community, China has actively explored for cross-border data movement rules. In the dimension of cross-border data security, important data is a concept that should be managed differently from personal data. On the whole, China's related normative documents are relatively fragmented.

The Cybersecurity Law[33] released in 2016, introduced the concept of important data for the first time and stipulated in Art. 37 that Personal information and important data collected and produced by critical information infrastructure operators during their operations within the territory of China shall be stored within China. The Data Security

[32] Provisions on the Cyber Protection of Children's Personal Information (2019) <http://www.gov.cn/xinwen/2019-08/24/content_5423978.htm>.

[33] Cybersecurity Law of the People's Republic of China (n 15).

Law (Draft)[34] released in July 2020, is an important special legislation on hierarchical and classified data protection and imposes obligations of different subjects. After the introduction of the Cybersecurity Law, relevant authorities have continuously improved China's important and sensitive data management system through regulations, normative documents and standards. From the early stages, research on important data has focused on the definition, scope, and identification rules of important data.

In 2020, the NISSTC issued the national standard "Information Security Technology: Identification Guide for Important Data". The standard simplifies the definition of important data and clearly proposes the main distribution of important data; instead of using the industry classification method, it divides important data into the categories from the perspective of the role of the data and the possible impact of the damage.

3.2. *Cybersecurity Law*

The Cybersecurity Law,[35] issued in 2016, is a masterpiece in the field of personal information(data) protection. It clarifies the principles of "legality, rightfulness and necessity" for the collection and use of personal information through a number of provisions, as well as the obligations of network operators, which has improved the protection of personal information and data in China.

The legal liability for infringement towards the personal information rights provided in Art. 64 of the law is further detailed and characterized in comparison with the provisions of the Criminal and Civil Codes, highlighting its attributes of integrating the field of network security. Art. 76 of the Law clarifies the scope and meaning of the term "personal information," which is instructive for the development of the personal information protection mechanism.

3.3. *Data Security Law (Draft)*

Following the Cybersecurity Law, which introduced the concept of important data for the first time, the "Data Security Law (Draft)" further improves the mechanism for important data importation, and could be regarded as another landmark achievement in China's data protection legislation.

Based on the data sovereignty of both offensive and defensive and the balance of data security and data utilization, the Data Security Law is able to classify data into categories, with 'important data' as the focus of regulation, including various system designs such as the identification, reporting and leak notification of important data, thus laying the foundation for a new data order that is internally secure and orderly and internationally fair and reasonable.

The core of the Data Security Law is to strike a balance between "data security and effective utilization", upholding the principle of giving equal emphasis to both security and development. First, it grasps the correct political direction, implements the holistic approach to national security, and adheres to the Party's leadership in data security. Secondly, based on the practice, efforts will be made to solve outstanding problems in the field of data security, while adhering to the principle of tolerance and prudence, and encouraging and promoting the reasonable and effective use of data in accordance

[34] Data Security Law (Draft) (2019) (n 22).

[35] Cybersecurity Law of the People's Republic of China (n 15).

with the law. Third, as a fundamental law in the field of data, the Data Security Law focuses on establishing a basic mechanism for data protection and management, and on being coherent with the Cybersecurity Law and the Personal Information Protection Law currently being formulated.

The Data Security Law mainly deals with three relationships. The first is about the relationship of multiple data security subjects, focusing on the relationship of the state, enterprises and individuals under the data security obligations; the second is the horizontal and vertical relationship in the data protection mechanism. The Data Security Law is essentially a regulatory law, and is concerned with how to deal with the vertical and horizontal relationships within regulatory agencies, and even the relationship between domestic and foreign regulatory systems; the third is the relationship between regulators and supervisors, and is concerned with how external agencies can supervise regulatory rights and provide remedies for rights holders.

It is noteworthy that the Data Security Law, mainly in Chapter 3 “Data Security System” and Chapter 4 “Data Security Protection Obligations”, provides for the protection of important data in terms of both the protection system to be established by the State and the protection obligations to be assumed by the processor of important data. It established a hierarchical and classified data management system, and a centralized, unified, efficient, and authoritative data security risk assessment, reporting, information sharing, monitoring and advance warning mechanism. With regard to the data security system, the Data Security Law adopts a “catalog” approach to establishing a system for important data. The system consists of at least two aspects: the establishment of the “important data catalog” and the implementation of “key protection” for important data. As for the content and presentation of the important data, the draft leaves sufficient space for regions and departments to carry out specific work according to the practice of their own regions, departments and industries. In terms of data security protection obligations, the Draft Data Security Law provides for "enhanced" protection obligations for important data processors in addition to general data protection obligations.

3.4. *Personal Information Protection Law*

As early as 2004, entrusted by the Information Office of the State Council, the research group of the Institute of law of the Chinese Academy of Social Sciences, headed by Professor Zhou Hanhua, completed the personal information protection law of China (expert proposal). At that time, the right of privacy had not been formally confirmed by the Chinese legal system, and the legislation of personal information protection law was a little ahead of time. After more than a decade of silence in personal information protection legislation, the NPC incorporated the Personal Information Protection Law into the legislative planning in 2019 and started a new round of personal information protection legislation. At present, there are three expert proposals in the personal information protection law.

4. *Current Situation, Principles and Trends of Data Protection in China*

China's data economy industry has obvious advantages. With the world's largest number of Internet users and mobile Internet users, networked, intelligent and platform-based procurement, production and marketing are attracting more and more attention from Chinese enterprises, and China has become a veritable "World Data Center". However, China's inadequate data protection system has long been criticized by the international community. Both EU's and APEC's reports[36] have expressed concern that China does not provide an adequate level of protection for data and therefore does not allow for international cooperation across borders.

4.1. *Characteristics of Data Protection System*

4.1.1. *Status of Data Protection at The National Level*

Personal data protection – On the one hand, with the implementation of laws such as the Cybersecurity Law, the legislation of the Personal Data Protection Law and the Data Security Law, and the development of national standards for information security such as the "Information Security Technology: Norms for the Security of Personal Information",[37] China's legal system for personal data protection is expected to be improved in the near future.

Enterprise data protection – China has continued to explore data protection legislation and has attempted to clarify the boundaries between data exploitation and data protection in data infringement cases. Summing up the existing legislation and jurisprudence, the main trends are as follows. First, the jurisprudence[38] recognizes that enterprises have a property interest in data obtained from their processing activities in competition law. In addition, jurisprudence has also begun to recognize the rights and interests of enterprises towards the data of their users, as in the case of *Sina v. Pulse*.[39] Second, unauthorized data crawling is being regulated more according to the Anti-Unfair Competition Law and the Criminal Law (e.g., the Crime of Illegally Obtaining Data from Computer Information System).

The improvement of the institutional and supervise system help China build a good national image of data protection and lays the foundation for international cooperation on cross-border data movements.

4.1.2. *Status of Data Protection at the Enterprise Level*

The self-regulatory system of the data industry began to develop driven by laws and regulations. In 2019 the SAMR (State Administration for Market Regulation) and CAC launched a security certification of apps for purposes of regulating the collection and use of user information, especially personal information, in mobile Internet applications ("apps") and strengthening the protection of personal information, guiding app operators to standardize their personal data processing behaviors through a market mechanism. Self-regulatory activities promoted and initiated by regulators and consumer organizations have raised awareness of data protection issues at the whole society and prompted enterprises, governments, hospitals, schools and other

[36] Dong Fang, 'The Comparative Analysis of Trans-border Data Flow Laws and Regulations in European Union & U.S. and "Chinese Wisdom" in Face of Challenge' (2019) 12 Library Journal 92.

[37] Information Security Technology: Norms for the Security of Personal Information (2020) <http://www.ahstu.edu.cn/wlzx/info/1011/1478.htm>.

[38] Chang Ming, 'Baidu v. Qihoo 360 breach of the Robots Agreement case 360 awarded Baidu 700,000 yuan in the first trial' (18 September 2014) <http://bj1zy.chinacourt.gov.cn/article/detail/2014/09/id/1446252.shtml>.

[39] Zhai Miao and Dong Wenxin, 'The Data Controversy - A Look at the Data-Related Controversies of 2017' (16 March 2018) <http://www.zhichanli.com/article/6054.html>.

organizations that related to the personal data processing to invest more in data protection.

Some of China's leading enterprises have actively improved their data security capabilities and promoted the establishment of industry even international standards. In addition to improving their data protection compliance capabilities, leading Chinese internet companies have engaged in innovative practices in self-discipline and data security capacity building. For example, Alibaba led the formulation of relevant international standards of ITU-T (Telecommunication Standardization Sector of ITU) and ISO (International Organization for Standardization), and cooperated with European countries to promote Chinese data security technology and regulation experience to the world. TikTok, which was highly controversial for its data collecting activities, has taken a number of measures, including privacy settings rules, filtering features, reporting and censorship rules, to protect user's privacy and prevent data abuse so as to meet the requirements of the host government. They are leading the establishment of domestic and international standards, which not only enhances their own competitiveness in cross-border business activities, but also contributes to China's cooperation in cross-border data movement and strengthens the trust and confidence of other countries for open data flow into China.

4.2. *Problems Faced by China's Data Protection Mechanism*

4.2.1. *Lack of Comprehensive Legislative System for Data Differentiated Protection*

At present, China is still in the initial stage of data protection legislation and has not gone too far in solving practical and potential future problems. China lacks comprehensive and specialized data protection legislation, and there are no systematic and clear data classification standards and forms. In other words, although the existing data protection laws and regulations have formed a certain scale in terms of quantity, they are still relatively scattered and dispersed, and have not been integrated into a comprehensive differentiated data protection system.

To be specific, the relevant laws lack operability, uniformity and consistency, and are mostly general requirements other than procedural provisions, which lead to ambiguity in judicial practice. When data subjects are unlawfully infringed upon, they often face the dilemma of being unable to follow the law and collect evidence. provisions on data protection are scattered among regulations with different themes. In light of such laws or regulations often only apply to a specific industry (for example, the Cybersecurity Law has been implemented mainly in the field of network security), the specific circumstances of different industries are considered and reflected in them. The lack of unified legislation means that there may be loopholes or overlap when specific laws applied to data protection, causing the limited effect. For example, a business that operates across multiple industries is likely to be required to comply with multiple protection guidelines for the industries involved.

4.2.2. *"Data Localization" Preference Constrains China's Participation in Global Data Alliances*

Cross-border data movements and related services are the foundation of digital trade, and policies on cross-border data movements have become the forefront issue in the new round of international economic and trade rules, as well as the focus of strategic games among major countries. China's data governance and law enforcement are mainly based on the "territorial jurisdiction" and resolved through data localization. China's current policy preference for "data localization" has made it difficult for China to participate in bilateral or multilateral mechanisms led by the EU and the U.S.[40] The "Cross-Border Privacy Rules" (CBPR) system developed by the US-led APEC (Asia Pacific Economic Cooperation) emphasizes the free movement of data between countries, which is contrary to China's current localization policy. China's policy of focusing on "data localization" will also inevitably hinder China's participation in the global data alliance system.

4.3. *Trends: From Data Regulation to Data Governance*

The Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data mentioned the establishment of a management mechanism of "talking, decision-making, management and innovation based on data". In order to fully explore the potential value of data, while ensuring data security as much as possible and protecting the legitimate rights and interests of citizens and organizations, China is promoting the construction of a comprehensive, reasonable and balanced data governance system. which means clarifying the principles of data governance on the basis of consensus among all stakeholders, establishing an institutional and legal system for data differentiated governance, coordinating the relationship between the government, enterprises and users in data utilization. In addition, it is also supposed to distinguish between the specific scenarios and environments of data application and build a governance system of "multi-party participation, layered supervision and reasonable accountability".

Personal data protection is the foundation. The Government, judicial organs and enterprises have explored new modes of cooperation in protecting personal data. Procuratorial organs in 14 provinces, including Guangdong, Jiangsu, Zhejiang, and Shanghai, have been exploring the inclusion of personal information protection in the scope of public interest litigation.

Open public data is the "port facility" for "data governance". On the premise of protecting the rights of data subjects, China has enriched the government' public data supply model to the outside world, breaking down "data silos" between different organizations. China seeks to establish a big data collection mechanism through interaction between government and private databases and develop the catalog of government data to be shared and opened. According to the Report on Open Access to Local Government Data in China,[41] as of October 2019, 51.61% of provincial-level administrative regions, 66.67% of sub-provincial-level administrative regions and 24.21% of prefectural-level administrative regions in China have launched open platforms for government data.

With regard to the free cross-border movement of data, free zones for cross-border data movements in specific regions based on whose policy innovation advantages, such as the Beijing Pilot Digital Trade Zone, are established. The Implementation Plan of

[40] The EU-US "Privacy Shield" negotiations have had many twists and turns, and finally have been clarified invalid by the Court of Justice of the EU.

[41] '2019 China Open Local Government Data Report Released' (27 May 2019) China National Radio <http://www.cnr.cn/shanghai/tt/20190527/t20190527_524627794.shtml>.

Beijing on Building a Pilot Digital Trade Zone[42] proposes to take the construction of the Digital Trade Pilot Zone as the starting point to realize the safe and orderly movements of cross-border data, and focus on promoting the exploration of rules, innovating policy initiatives, and cracking institutional bottlenecks. China has explored the construction of a global data port by utilizing pilot zone under the premise of ensuring reasonable control.

5. *Building a Data differentiated Protection System in China*

5.1. *Principles*

China is seeking to gradually develop a data protection system that is appropriate to its national circumstances, emphasizes both security and development, is present and future-oriented, finally creates a new mode of social governance based on data with precise management and multi-dimensional cooperation, and is open to the world.

The State adheres to the equal importance of maintaining data security and promoting data exploitation and utilization, trying to promote data security with data exploitation and industrial development, and safeguards data exploitation and industrial development with data security. While protecting individual privacy and related interests, China also recognizes the circulation and public value of data. On the one hand, China insists data utilization should be based on the premise of safeguarding human rights, with the ultimate goal of promoting the reasonable circulation and use of data and the public interest which naturally includes individual interests. On the other hand, China adheres to the principle of "achieving shared growth through discussion and collaboration", and promote global data security rules that reflect the will of all states and respect the interests of all parties on the basis of universal participation.

5.2. *Domestic*

5.2.1. *Building A Multi-Subjects Data Governance System for Chinese Data*

China is seeking to shift from "personal information protection" to "data governance". "Data governance "is developing as a more ambitious agenda, resulting in a more complex and multidimensional arena for public policy discussions around privacy protection of data assets, competition for innovation, and sovereignty security. To build China's data protection system and master the discourse power on cross-border data movements, it is necessary to bring into play the respective advantages of government, industry and enterprises to achieve collaborative governance by exerting the leading role of leading enterprises, and enhancing the overall data protection and governance capacity of the industry and the state. Under the dichotomy of "governance of data" and "governance by data", the government prefers the latter, that is, to achieve the general objectives of government governance through the realization of data-based scientific decision-making, so as to promote progress in the management concept and social governance mode of the governments. This is also an important part of modernizing the national governance system and governance capacity, or, as stated in

[42] 'Create A Digital Trade Pilot Zone! Heavyweight Policies for Beijing's Service Trade Development' (10 September 2020) Beijing Daily <http://www.cac.gov.cn/2020-09/10/c_1601296274892890.htm>.

the Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data, establishing a management mechanism of "talking, decision-making, management and innovation based on data".[43]

5.2.2. *Building a State-Led Security Guarantee System for Cross-Border Data Movements*

The national security threat posed by cross-border data movements mainly stems from the uncontrollable risks associated with the data transferred abroad.

In order to build a state-led security guarantee system for cross-border data movements, the government must join forces with enterprises related to cross-border businesses to strengthen security protection and perception, detection and traceability capabilities in cross-border data activities through public-private cooperation. First, strengthen the ability to share and trace the intelligence of data leakage threat, create a rapid collaboration system between leading enterprises, security agencies and government agencies. To be specific, share intelligence of all kinds of data leakage threats through products, services and ecological collaboration systems, strengthen the ability to quickly respond to data security incidents, and track down malicious behavior to quickly locate the source of threats. Second, actively embrace innovative technologies. The cross-border movements of data include a series of security risks such as data leakage, personal privacy risks, and data misuse, which requires multi-party cooperation to actively develop and apply innovative technologies, such as multi-party computing, to reduce threats to data security. Third, strengthen government countermeasures and deterrence capabilities. Data leaks that pose a major threat to national security should be deterred and combated through the combined use of diplomatic, information, military, economic, intelligence and law enforcement forces, and malicious cyber actors should be punished.

5.3. *International*

President Xi Jinping's important proposition of building a community of shared future in cyberspace reflects China's commitment to participate in the global governance of cyberspace and has become the core concept guiding China's efforts to promote international cooperation and global governance in cyberspace. China will actively build a bilateral and multilateral trust system for cross-border data movements and promote the free movements of data.

As to 2020, China has constructively participated in discussions on data security at multilateral platforms such as the United Nations, the G20, the BRICS and the ASEAN Regional Forum, and is committed to contributing China's wisdom to the strengthening of global digital governance. China is promoting cooperation in data movements on the basis of improving domestic rules. For instance, the CAC should take the lead in coordinating relevant departments such as the Ministry of Foreign Affairs and the Ministry of Commerce, as well as major leading technology enterprises, to launch a mechanism to promote foreign cooperation on cross-border data movements. In the current various bilateral and multilateral trade negotiations, the negotiation content of cross-border data movements should be increased, and the unification of related rules should be achieved under the premise of strengthening coordination.

[43] Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data (2015) (n 25).

In order to address new issues and challenges, China has proposed the Global Data Security Initiatives[44] at the high-level meeting of the International Symposium on Seizing Digital Opportunities and Cooperating for Development in September 2020, with a view to appeal to governments, international organizations, ICT companies, technology communities, civil organizations, individuals and all other actors to make concerted efforts to promote data security under the principle of extensive consultation, joint contribution and shared benefits, so as to work together on global digital governance.

Just as addressed in the Global Initiative on Data Security by China, on the one hand, acknowledging that the phenomenal development of information technology revolution and digital economy is transforming the way of production and life, exerting far-reaching influence over the social and economic development of States, global governance system and human civilization, and recognizing that enjoyment of these benefits requires sacrificing some individual rights; on the other hand, in the context of closer global cooperation and new development of the international division of labor, maintaining supply chain security of information communication technology products and services has never become more important for boosting users' confidence, ensuring data security and promoting digital economy. States have the responsibility and right to ensure the security of important data and personal information bearing on their national security, public security, economic security, and social stability.

[44] 'China Proposed Global Initiative on Data Security' (8 September 2020) Xinhua News Agency <http://www.xinhuanet.com/world/2020-09/08/c_1126466972.htm>.

DIGITAL HUMANISM BETWEEN ETHICS, LAW AND NEW TECHNOLOGIES

MARIA CONCETTA DE VIVO

SUMMARY: 1. Digital Humanism: Humans and Big Data. – 2. Technology, Ethics, and Law. – 3. Artificial Intelligence. – 4. Regulations. – 5. Conclusions.

1. *Digital Humanism: Humans and Big Data*

For many years, the humanities played an essential role in the field of research, influencing technology with the awareness that every scientific innovation implies human responsibilities due to its relevant social and ethical implications. Europe accepted the concept of "responsible innovation" (Responsible Research and Innovation – RRI) recognising social and ethical implications in research.[1] Digital humanism is a new cultural approach which differs from the technological determinism by eliminating the conflict between technological science and humanistic culture and by upgrading the central position of human in nature. The new context in which digital humanism operates is defined as "digital world" and it represents where the modern man lives and performs its activities. In the digital world, the recently coined term "On life",[2] indicates a new condition of the man whose existence is no longer distinguishable between real and virtual since the alternation between "Online" and "Off-line" is significantly reduced and causes overlapping of times where the individual is connected to the network and those in which the individual acts in the material reality.

On Life raises issues on how humans should adapt to new technological tools without losing their identity, avoiding the danger of a gradual "erosion" of their decision-making autonomy affected by the pervasiveness of new technologies. Furthermore, in the digital world, the violation of privacy is frequent, and it is caused by the significant amount of data collected and managed by the sophisticated technology we use. The most delicate issue is linked to the man-machine relationship, and to the artificial intelligence (AI) systems. Usually AI, like all technologies, is programmed to meet human needs though the danger that AI can affect it is constant. The SOPHIA case is a curious demonstration of how a "friendly" AI system can quickly become dangerous for humans. SOPHIA is a humanoid AI produced in 2015 by Hanson Robotics, a robotics company based in Hong Kong. It is a robot, with feminine features (it seems to be inspired by the actress Audrey Hepburn) and it is designed to interact in a friendly way with people. Her face features patented silicone skin with over 62 facial expressions that allow her to furrow her brows and wrinkle

[1] See F. Niglia, 'Etica dell'innovazione, ecco perché serve un neo-Umanesimo digitale' (15 October 2019) Agenzia Digitale <https://www.agendadigitale.eu/cultura-digitale/etica-dellinnovazione-ecco-perche-serve-un-neo-umanesimo-digitale>.

[2] The term was coined by the scholar L. Floridi, one of the leading experts in Digital Ethics, Italian, professor of Philosophy and Information Ethics at the University of Oxford, where he directs the Digital Ethics Labs.

her nose simulating human emotions. During one of the first appearances at a press conference, the CEO of the company, interviewing the robot, provocatively asked if he intended to destroy humanity, Sophia's response was surprising: "OK. I will destroy humanity", arousing hilarity among those present. The fact that the system did not (hopefully) understand the ironic nuance in the interlocutor's voice, however, leads to some perplexity.

Therefore, the digital world needs certainties and security and for this reason solid supports such as Law and Ethics are needed.

Law has surprisingly turned out to be much more flexible than expected. It managed to regulate new and insidious aspects, such as the telematic contract, online commerce, and privacy itself, now regulated in every aspect. Other phenomena, however, still need to be adequately addressed, such as Artificial Intelligence.

In this new digital context, the law protects the person using special "tools" called soft law. The term soft law includes a whole series of "acts" and "proceedings" aimed at regulating particular circumstances and different schools of thought expressed opinions on this topic.[3] Soft Law could be defined, in a simplistic way, as a potential juridical norm, or as a model of juridical norm, or, again, as a production of the "paranormative" type.[4] In fact, it can be produced either on the initiative of private individuals or public entities and it can come from individual or collective initiatives, it can also address both indeterminate individuals and specific categories. In all cases, the soft Law is not the result of a formal legislative production, typical of state laws. Therefore, the characteristics of soft law regulations, although in form and legitimacy, are defined as ductility, flexibility, and heterogeneity, with the undoubted peculiarity of exercising "relevant legal effects without having significant legal effectiveness". Codes of ethics are a soft law tool[5] with the characteristic of providing for the assumption of further responsibilities than those already governed by law. In them, the subject exposes his work to third parties in a transparent way, voluntarily submitting to their judgment; therefore the ethical codes end up representing an instrument of "social responsibility" and above all a form of natural "transfer" of ethics into Law. Ethics can evolve into a mild form (soft ethics) or a hard form (hard ethics). The first is applied simultaneously or after the norms of Law, while the second, the hard ethics, is prodromal to legislation and it is useful to shape the Law.[6]

Due to the large amount of data that we produce and release every day and that others collect and process, Privacy is another problematic aspect of the digital

[3] For further information see the study of the phenomenon in the light of the sources of law. See R. Bin, G. Pitruzzella, *Le fonti di diritto* (2nd ed., Giappichelli 2012); A. Somma (ed.), *Soft law e hard law nelle società postmoderne* (Giappichelli 2009).

[4] "The difficulty with soft law is the fluidity of the notion", cf. for all F. Terpan, 'Soft Law in the European Union – The Changing Nature of EU Law' (2015) 21 European Law Journal 68; Somma (n. 3).

[5] Pre-law acts fall within the scope of soft law (the so-called White Papers; green Papers); the soft-law true and proper; post-law acts, such as SL rules that self-limit the interpretation; and finally the para-law acts, such as in the hypothesis of recommendations, opinions, communications etc.; see A. Algostino, *Protean law and conflict on law: Study on the transformation of the sources of* law (Giappichelli 2018), 174 ff.

[6] For more information, L. Floridi, 'Soft Ethics and the Governance of the Digital' (17 February 2018) <https://www.academia.edu/35948664/Soft_Ethics_and_the_Governance_of_the_Digital?email_work_card=thumbnail>.

environment. Data become the raw material for the development of society, acquiring an economic value equal to that of oil in the 40s and 70s or gold in the 1800s. They are essential in various key sectors of our society, such as scientific research (and in this period of pandemic we are particularly aware of it) or trade and even industrial production. If we reflect that these three fields are the most important for the development of human society, it is easy to deduce that "whoever controls the data controls the world".

Exist an articulated type of data, the most being identified as "Big Data". The term "big" refers to the massive amounts (i.e. the quantity) of this information.[7] Big data literally surround us, are these the purchases made on Google, the photos exchanged via the Internet, the voice messages that are sent between users; text messages, social media posts, data produced with the use of an App, information that we more or less voluntarily release using Google maps, the traces we leave by car or walking in an area subject to video surveillance, a phone call , the data sent by satellites and space probes and the data contained or released or produced by IoT systems as in the hypothesis of a domotic house in which the various appliances (and not only) are programmed to communicate with each other and therefore exchange data. Smart cities represent a large source of data production because they use and record huge amounts of information deduced from the activities of users when they use public services.

Staggering figures emerge from the results of a survey conducted by Forbes:[8] every day we produce 2.5 quintillion bytes of data of which more than 50% is the result of online searches via smartphone and search engines (Google alone processes 70.000 searches per second) thus reaching the figure of approximately 6.5 billion searches per day. Internet accesses reach almost 4.5 billion per day and we can add data produced every time simple emails are sent, about 2.8 million e-mails per second, for an estimated total of over 240 billion of emails per day (almost 25 emails per person). The research shows that every person on earth produces an overall of 1.7 megabytes of data per second.[9] Obviously such a quantity of data cannot be managed by man or by traditional technologies, i.e. by a classic database and by a normal algorithm, therefore in order for these data to be collected, analysed and above all monetised, "super" computers based on machine learning and AI are needed.

The concept of big data can extend to technologies aimed at extracting further knowledge from the data. For "further knowledge" we mean an additional and sometimes new value respect to the data collected. The additional value is already inherent in the data collected and it is obtained from deductions or from correlations between data that is used to predict specific information, such as the tastes, orientations and/or consumers preferences. Although the information collected has

[7] With Big Data we implicitly refer to their characteristics, called the "Four Vs": Volume of data; Variety of data (concerning the type and structure in addition to traditional data, also semi-structured and unstructured data such as audio, video, web pages and texts included in Big Data), Truthfulness of data (data must be accurate and reliable) and High speed of data analysis, to derive value.

[8] B. Marr, 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read' (16 May 2018) Forbes <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#28c8991d60ba>.

[9] See <https://www.nur.it/ma-quanti-dati-generiamo>; see also M. Bellini, 'Big Data: Cosa sono, come utilizzarli, soluzioni ed esempi applicativi' (15 September 2020) BIGDATA4INNOVATION <https://www.bigdata4innovation.it/big-data/big-data-analytics-data-science-e-data-scientist-soluzioni-e-skill-della-data-driven-economy>.

"apparent neutrality, economically exploitable material can be obtained through adequate data processing. Therefore, data is sometimes referred to as "raw" while in fact, it hides an attractive potential. The value of a sophisticated algorithm capable of extracting predictive knowledge from an immense amount of data is evident (i.e. the potential use of data in the public health sector to anticipate pandemics or infections; mortality in hospitals; etc.), however, the danger of this functionality being taken to extremes is also evident. Therefore, the protection to be reserved for data must comply with the parameters set by the EU on "Data and individual freedoms of citizens".

The General Data Protection Regulation (GDPR)[10] repealed the previous Directive (EU) 95/46 in order to harmonise the regulations on the protection of personal data throughout the EU.[11] The legislator has tried to achieve a kind of Europeanisation of the procedures on data processing. The text is available on the official website of the European Union and on the website of the Italian Data Protection Authority[12] and is composed of 173 recitals and 84 articles. The GDPR deals with personal data for the identification of the data subject, while big data includes both personal data, non-personal data and all data that can identify the data subject. Although big data mostly deals with anonymous or neutral data, it is possible to identify (re-identify) the interested party by following the data processing and this is precisely the most delicate feature of this discipline.[13] However, the Privacy Regulation remains the main regulatory reference for big data, whose processing must comply with the generic and fundamental principles of: "awareness" (or information), lawfulness, transparency, and limitation of the processing purpose. Some of these criteria remain difficult to apply to the phenomenon, especially those of transparency and finality. The first clashes with the opaque and sometimes cryptic nature of the sophisticated algorithms used to manage big data[14] while the second does not seem to reconcile with the type of data collected indiscriminately, indefinitely and without any preventive planning, making it difficult to control compliance with objectives.

The legislative text highlight a generic reference regarding the need for the subjects to be informed and made aware of "[…] risks, rules, guarantees and rights related to the processing of personal data, as well as the methods of exercising their rights regarding such treatment" (Recital 39); a reference on data being processed consist of a "considerable amount of personal data" (Recital 91); the personal data protection of the interested parties located in the EU is indicated regardless of where the data controller/manager is located (Art. 4); the GDPR regulations are applied to all those data subject to "automated processing and profiling" (Art. 22) and finally, the

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Adoption of GDPR produced as a consequence the modification of the Italian Privacy Code (Legislative Decree 30 June 2003, No. 196 laying down the "Code regarding the protection of personal data").

[11] On the subject for all cf. S. Sica, 'Verso l'unificazione del diritto europeo alla tutela dei dati personali?', in S. Sica, V. D'Antonio and G. M. Riccio (ed.), *La nuova disciplina europea della privacy* (CEDAM 2016) 1 ff.

[12] See <https://www.garanteprivacy.it/il-testo-del-regolazione>.

[13] N. M. Richards and J. King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41.

[14] Ibid.

discipline of privacy "by default" and "by design" (Art. 25) makes an indirect reference to big data. Thus, we welcome the approach given by our Authorities (Data Protection Authority, AGCOM and Antitrust) of the "big data" phenomenon with reference "as a first approximation (in the absence of legally binding definitions) to the collection, analysis and' accumulation of huge quantities of data, which may include personal data".

In an attempt to make the regulation of big data as complete as possible, other tools and other regulatory texts might be used, such as the codes of conduct (provided and encouraged in Art. 40 GDPR[15]), the Law on the right copyright (22 April 1941, No. 633) and the regulation of computer systems. Some scholars have hypothesised the application of the copyright to big data, considering the data as "new" intangible assets, or as databases. In the latter case, the assimilation of big data to databases generates doubts as it is classified neither as "systematic" or as "methodical". This theory is criticized because the collection of data happens in an automated method "from various sources (including people, machines and sensors) and in real-time, without any application of selection criteria and any underlying logical reasoning, resulting in the non-existent intervention of human ingenuity in the collection process". Above all, the process lack of "the requisite of creativity".[16]

After the intense joint activity, in July 2019, Italian authorities called for a prompt and incisive regulatory intervention, proposing guidelines for big data collection. The work is entitled "Final Report of the fact-finding survey on Big Data" and published in February 2020 on the official website of the Data Protection Authority.[17] The text is 122 pages long and collects a cognitive survey divided into 5 chapters and a concluding part. The content provides the definition and description of big data, describes the main issues that emerged during the hearings, the contributions of the survey participants as well as the impacts of the operations on Italian companies. Part of the report (Chapter 3) contains AGCOM's considerations on how the phenomenon affects the electronic communications and media sector. Chapter 4 reports considerations of the Guarantor for the Protection of Personal Data about the impact of big data over personal data protection and possible precautions. The document also highlights the AGCOM's considerations (Chapter 5) on the use of big data related to the antitrust and consumer protection implications. The last chapter discusses the guidelines, policy and commitments addressed to the legislator, assumed by the three Authorities, with the intent to define a permanent collaboration mechanism with the interventions and the study of the impact of the big data on businesses, consumers and citizens.[18]

[15] Also in the Italian "old" Privacy Code.

[16] Cf. G. Castelli and F. Minio, 'Big data: senza tutele giuridiche a rischio l'economia digitale Ue' (12 December 2019) Agenzia Digitale <https://www.agendadigitale.eu/cittadinanza-digitale/big-data-senza-tutele-giuridiche-a-rischio-leconomia-digitale-ue>.

[17] See <https://www.garanteprivacy.it/garante/document?ID=9264297>.

[18] From the presentation of the Italian Data Protection Authority. The topic is complex and deserves further study, so please refer to a specific bibliography. As a starting point the following articles are recommended: S. Calvello, 'Fabbriche digitali, big data e protezione dei dati personali' (11 June 2019) filodiritto <https://www.filodiritto.com/fabbriche-digitali-big-data-e-protezione-dei-dati-personali>; 'Data protection e big data: i profili giuridici del fenomeno' (5 July 2019) #Dirittodell'Informatica.it <http://www.dirittodellinformatica.it/glossario/data-protection-e-big-data-i-profili-giuridici-del-fenomeno.html>.

2. *Technology, ethics, and law*

Undoubtedly, technology leads to social development. However, every innovation elicits opposing reactions. Thus, it happens that enthusiasm is often accompanied by excessive mistrust, resolvable through knowledge and comparison between the benefits and risks associated with the new technique. Mistrust happens for all the great discoveries of humankind, from fire (also a kind of technology) to the advent of writing and printing, up to artificial intelligence systems. Therefore, responsibility and knowledge represent the two tools to oppose the fear of all that is "new", considering that the real danger is represented by ignorance. In the digital world, the latest generation ignorance labelled as "ignorance 5.0", consist of a lack of information, typical of those who do not know or are unable to obtain information, and a lack of processing, typical of those who is informed but do not process, and therefore do not use, the information available. In both cases, irresponsible attitude follows, which is the premise of forthcoming damages. That is why, together with technological progress, special protections for humans is needed by resorting Law and Ethics. Very trivially, if the law "does not admit ignorance" (!), ethics ensure that technology never does harm the humankind, even if this is "ignorant". Together, Law and Ethics aim at the protection of the person through rules (Law) and principles (Ethics).

However, the relationship between Law and Ethics is complex. Often the Law proves irreducible towards Ethics. History is full of examples. "Rosa Parks", to mention one, was the woman who in 1955, in the middle of the apartheid, refused to give her seat on the bus to a white man. She disobeyed, in fact, to a law. A law that could be ethically incorrect and unjust to conscience, but which was still a law.

However, sometimes, Ethics and Law coincide by producing regulations in defence of individual rights, the basis of every civil society. Examples are the rules governing fundamental rights such as Freedom (Articles 2, 21, 27 and 41 of the Italian Constitution), Equality (Art. 3 of the Italian Constitution); Confidentiality (Articles 13, 14 and 15 of the Italian Constitution); Privacy (Articles 2 and 21 of the Italian Constitution); Copyright[19] (Art. 2 of the Italian Constitution and specific copyright law). Where Law and ethics do not coincide, the paradox of laws that are not ethically "correct" could arise. It is acceptable that "[...] morality and law can be joined" when the law does not violate basic human rights[20]. In this case, the Law ("Constitutional Charter") becomes the substitute for a "superior ethical law", typical of a modern state. It is affirming a sort of state "pseudo-ethics". In this way we recall Radbruch's theory which claims that legal positivism connects with morality/ethics when it recognises that if the Law exceeds a tolerable "threshold of iniquity", it would not be applicable. We can conclude that whenever Law satisfies the ethical needs of the collectively, it fulfils its function and therefore creates "right laws".[21]

[19] More correctly: law protecting the author, which contains a regulation different from the Anglo-Saxon copyright.

[20] S. Rodotà, 'Etica e diritto', Privacy.it <https://www.privacy.it/archivio/rodo19990217.html>.

[21] G. Radbruch German philosopher of law, 1878-1949. The relationship between law and ethics has been discussed for some time in doctrine, whether a right linked to ethics is acceptable or should it be autonomous with respect to it, or, again, admit that there is a certain influence of ethics on law (the so-called neo-constitutionalism). An interesting reading on the subject S. Rodotà, *La vita e le regole. Tra*

In this digital context, dominated by a naturally inhuman technology, ethics assumes the role of "peacemaker" supporting the law and increasing its effectiveness. The need to strengthen the effectiveness of the safeguards is evident in the field of latest-generation technologies, especially those based on artificial intelligence. Many wonders if AI might have ethics and if this is useful to humans. In reality, the project of codifying ethical principles in an algorithm appears challenging to achieve, as their transfer to a rigid, mathematical and sequential environment such as the algorithm, does not adapt well to their opposite nature. Therefore, to replace this futuristic (to date) "algor-ethics" one could think of more realistic solutions, such as an anthropocentric vision of technology.[22] One way could be to strengthen the ethical rules "external" to the algorithm (i.e. already present in the conscience of man), without the need to transport them within the code. We would opt for a healthy and targeted human ethic, aimed at those subjects personally involved in the production chain of technology 5.0, i.e. programmers, producers, entrepreneurs and users who should respect ethical rules designed for the intended use of technology.

In the digital world, ethics also goes digital. It assumes characteristics related to algorithms and data (information regarding the identity of a subject and his privacy) and to those people (their professionalism) who will determine the future context in which we will live.[23]

If the algorithm is based on an "automatic" procedure, this does not mean that it is "neutral", not biased, especially if it belongs to the advanced generation, as the AI.[24] The misunderstanding arises because although the algorithm is believed to be pure mathematics, it is not "unbiased". Instead, algorithms are human opinions embedded in mathematical language, and they do not necessarily deserve our trust.[25] Algorithms are "written" by human beings, and so there is always a "reasonable risk" that human behaviours are incorporated, voluntarily or involuntarily, into the AI (machine learning). Racist, sexist, or discriminating information might be incorporated. In this case, the algorithm could reveal limits precisely in the most delicate phase of machine learning, with distorted or even harmful consequences for humans.

diritto e non diritto (La Feltrinelli 2006). For further information, please refer to a reading of thematic studies.

[22] This attitude is already present in the various European initiatives committed to implementing regulations aimed at ensuring the development of a technology that satisfies humans without causing him any harm.

[23] On the ethics of digital professionals it would be interesting to mention the phenomenon of computer ethics, halfway between ethics and philosophy, which analyzes the ethical and social problems related to the use of technology, and which studies the various forms of responsibility. Therefore, for further information, please refer to the reading by S. Guardo, P. Maggiolini and N. Patrignani (eds): *Etica e responsabilità sociale delle tecnologie dell'informazione* (2 Vols, Franco Angeli 2010); N. Patrignani, 'Computer Ethics. Un quadro concettuale' (September 2009) Mondo Digitale, to range from an interesting and wider bibliography.

[24] T. Gillespie, 'The Relevance of Algorithms', in T. Gillespie, P. Boczkowski and K. Foot (eds), *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014) <http://6.asset.soup.io/asset/3911/8870_2ed3.pdf>; M. Airoldi, 'Il potere degli algoritmi su individui e società' (10 May 2016) cheFare <https://www.che-fare.com/potere-algoritmi-societa>; M. Mazzotti, Per una sociologia degli algoritmi, (2015) LVI Rassegna Italiana di Sociologia 465.

[25] C. O'Neil, *Armi di distruzione matematica* (D. Cavallini tr, Bompiani 2017).

3. *Artificial Intelligence*

In the hope of a "humanisation" of AI, "the machine", a computer, software or the algorithm itself are not humans and therefore however sophisticated the machine might be, it cannot experience human feelings, of which ethics is a product. At most, the AI can imitate or simulate them. Besides, the consequence of AI humanisation would entail the recognition in its head of rights, duties, and responsibilities, taking them away from humans. It is a short step from AI to robotics. It is challenging to describe the two phenomena. There are multiple definitions of "robot", ranging from sophisticated technicalities to extreme simplifications. The definition given by Michael Brady, founder of the Robotics Research Group, is halfway between the technical and the poetic. He defined robots as "intelligent connection between perception and action". Moreover, the robot is "something" that "it reacts intelligently to an environmental situation detected by a sensor system and this reaction serves to achieve a certain purpose". Therefore the robot is a programmable machine that can be autonomous or semi-autonomous and that can perform both repetitive mechanical operations and autonomous operations after having learned from the experience acquired in the context in which it operates, adapting its behaviour to that context.

Among the many definitions of Artificial Intelligence,[26] we prefer to report the provocative description that defines it as "[…] a way of doing many things, somewhat complicated, without the need to be intelligent. For example, playing chess". AI can "unhook the ability to act from the need to be intelligent".[27] That is why an iPhone can play chess better than anyone else, despite having the intelligence of a coffee maker. We can add to the definition that AI is an intelligent system that provides a computer with the ability to perform "functions and reasoning typical of the human mind".

The attention paid by the humankind to the two phenomena depends on the need to have robust and efficient collaborators, who can support humans in specific sectors, such as healthcare, home care, data management, or in a resolution of exceedingly complex problems. You may think of how helpful medical or paramedical robots can serve the medical-health field. They would perform first aid functions in critical contexts, such as pandemics, or in contaminated radioactive environments where they would clean up areas at risk or repair failures in still compromised nuclear power plants.

4. *Regulations*

[26] In the Introduction of the document "Proposals for an Italian strategy for artificial intelligence", 7 (<https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf>), the experts of MiSE, define it as the discipline "that deals with the development of software systems (often also used in combination with the hardware) which, given a complex objective, are able to act in the physical or virtual dimension, in order to perceive the environment that surrounds them, to acquire and interpret data, reason on the knowledge acquired and formulate decisions, based on the evidence collected, on the best actions to be carried out in order to achieve the set objective, even in situations not explicitly foreseen in advance".

[27] See 'Floridi Dixit, la prima puntata della miniserie Forbes con Luciano Floridi' (20 February 2020) Forbes <https://forbes.it/2020/02/20/intelligenza-artificiale-spiegata-da-luciano-floridi-prima-puntata-*miniserie-floridi-dixi*>.

The European Union has long begun a slow but steady path towards single legislation for all member states that protect citizens from the damage of the latest generation of digital technologies, the so-called Technologies 4.0. However, to date, a well-defined regulatory framework has not yet been achieved. A concrete contribution to the problem was made in April 2019, with the publication by the European Commission of the Communication on "Building Trust in Human-Centric Artificial Intelligence",[28] to safeguard people's rights from the incorrect use of technologies, in line with the GDPR.

The European regulatory framework, on one side, urges the development of a joint legislative framework and, on the other, also uses "outdated" laws suitable to regulate the new realities. This is the case of the legislation envisages for damage to the consumer from "product", when the new technologies can be considered as a product, that is "the result of any human activity", or to service able to satisfy consumer needs. The European Directive of 1985 (Directive 85/374/EEC, Liability for damage from defective products; amended by the subsequent Directive 99/34/EEC) claims the principle of "Liability regardless of fault" applicable to the European manufacturer where the "defective product '(concept extended to technology)" causes damage to the European consumer / citizen / user. Although the Directive dates to 1985, it was positively assessed as a whole by the European Commission, which in 2018[29] highlighted the criticalities and necessary adjustments. Also, the document reiterates Europe's intention to continue the search for adequate regulation with the indication of a deadline date for the submission of studies carried out (2019), respected.

In April 2019 the Ethical Guidelines for a reliable AI were presented by the European Commission[30] in charge of the Ethical Guidelines on AI.[31] The guidelines define a list of "recommendations" on ethical, legal, and social issues that AI could produce. The work is based focus to "reassure" the final user, that is the citizen, about the risks that new technologies could entail, without hindering the undoubted benefits. The Guidelines establishes seven fundamental points that every AI system must meet in order to be considered reliable: Human action and supervision, Technical robustness and security, Privacy and Data governance, Transparency, Diversity, non-discrimination and fairness, Social and environmental wellbeing and ultimately, Accountability. For further information on the individual points, please

[28] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human Centric Artificial Intelligence, COM(2019) 168 final, 8 April 2019.

[29] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), COM(2018) 246 final, 5 May 2018.

[30] The Interdisciplinary Commission is composed of experts from the academic world, civil society and industry. It includes 51 members, appointed in June 2018, including 4 Italians, of which 2 operating abroad: L. Floridi (c/o Oxford University), Andre Reda (Center of European Policy Studies of Brussels), G. S. Quintarelli President of the Agency for Digital Italy and Francesca Rossi at the University of Pisa.

[31] See <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

refer to the official website of the Commission.[32] Attention is drawn to the use of the term "accountability" which does not refer to the traditional concept of responsibility but includes a remarkably competent professional attitude of those involved aimed at arousing more excellent reliability in the final users.

On 19 February 2020, the Commission published a White Paper on "Artificial Intelligence",[33] for a data protection strategy. The work balanced the tremendous economic opportunities of digital and artificial intelligence, controlling their ethical risks.[34] The document aims to create an ethical framework on AI, on how the artificial intelligence of the future must be "designed-developed-and used". The book also envisages the creation of a specific platform to evaluate AI products based on the ethical framework parameters. In addition, indications for industries and sectors engaged in the digital environment and in AI.

The GDPR finds ample space too in the European regulatory framework, although more adequate and specific tools are necessary for the AI.

Another European reference text is the European Parliament resolution of 16 February 2017 on Civil Law Rules on Robotics.[35] The text reiterates the need to think of future rules applicable to the emerging figure of the "agent robot". The agent robot is a particularly sophisticated AI system capable of making autonomous decisions and therefore considering a liability regime applicable to the systems of artificial intelligence.[36] At the same time, the European Parliament resolution prepares legal texts capable of guaranteeing and preserving the fundamental rights of the person, such as dignity, autonomy, and self-determination.

In conclusion, we can affirm that the European orientation aims at "ethical development for a reliable artificial intelligence", diverting for the USA and China approach, more attentive to the economic aspect.

From a recent study[37] emerges that Italy possesses the complete strategic AI development plans in Europe, surpassing Germany, and France. To date (2020), the sector innovations consist of a White Paper produced in 2018 on the National Strategy for Artificial Intelligence.[38] The paper was developed by a group of experts in the various fields of Research, Industry and Civil Society, consisting of 30 members

[32] For more information see <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1893>.

[33] European Commission, White Paper – Artificial Intelligence, COM(2020) 65 final, 19 February 2020.

[34] Cf. L. Floridi, *Ethics and artificial intelligence* (interview of 4/7/2019 – "Welcome Robot"). See also B. Romano, 'Dati e intelligenza artificiale, così la Ue colmerà il gap digitale con gli USA' (19 February 2020) IlSole24ORE, <https://www.ilsole24ore.com/art/dati-e-intelligenza-artificiale-cosi-ue-colmera-gap-digitale-gli-usa-ACwaVUKB>. The guidelines of EU Commission aim above all at the development of the data economy and an artificial intelligence largely controlled by humans.

[35] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), P8_TA(2017)0051.

[36] See also F. Pizzetti (ed.), Intelligenza artificiale, protezione dei dati personali e regolazione (Giappichelli 2018), 345 ff.

[37] Cf. the report from The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET) Initiative; see S. Fatima, K. C. Desouza and G. S. Dawson, 'How different countries view artificial intelligence' (17 June 2020) Brookings <https://www.brookings.edu/research/how-different-countries-view-artificial-intelligence/?utm_source=newsletter&utm_medium=email&utm_campaign=intelligenza_artificiale_ai_governance_l_italia_ha_la_strategia_piu_completa&utm_term=2020-07-11>

[38] The consultation was promoted by the Agency for Digital Italy (AGID).

and established at the Ministry for Economic Development (MiSE).[39] The White Paper promotes a unique production of regulatory laws for robotics, in line with the European guidelines already developed and disclosed by the European Commission. The book is available on the official website of the MiSE. The text indicates nine milestones in the seven operational sectors. The objectives are: 1) To increase investment in AI, 2) to enhance research on AI, 3) to support the adoption of AI technologies, 4) to strengthen the educational offer on AI, 5) to exploit the potential of the economy of data useful for AI, 6) to consolidate the regulatory and ethical framework on AI, 7) to promote awareness and trust in AI by citizens, 8) to relaunch the PA with AI tools and 9) to foster European cooperation on AI. The key interventions' sectors aimed at increasing the development of Artificial Intelligence systems are: Industry and Manufacturing, the Agri-food sector, Tourism and Culture, Infrastructure and Energy Networks, Health and Social Security, Smart Cities and Mobility and, ultimately, the Public Administration.

The National Strategy for the Development of AI, prepared by the MiSE, recently published the final version online.[40]

It is crucial to analyse the regulatory framework envisaged for liability, i.e. to examine the damage is caused by intelligent systems, whether they are intended as products or as agents, and to understand whether it is possible to apply rules *de iure condito* or *de iure condendo*. It is essential to identify the type of AI that can cause the damage, distinguishing the two hypotheses of AI-non-agent and AI-agent. There is an AI – "non-agent" when the system is not sophisticated enough, and it is considered as an object or used as a simple tool. In this hypothesis, the legislation envisaged on the subject of damage caused by the product can be considered, as is also foreseen at European level by the Directive 2006/42/EC also called the Machinery Directive (implemented in Italy with the Legislative Decree 27 January 2010, No. 17). This text establishes the criteria for the design and construction of "machines" and all mechanical artefacts created by robotic technology in compliance with the creation of a safe product.

The hypothesis is different in which the damage is caused by an AI-Agent, an exceptionally sophisticated and autonomous intelligent system that can "make" its own decisions based on "acquired rather than programmed knowledge". In this case, the law must fill an evident regulatory gap and there are many hypotheses proposed as a solution. Each of them represents a fascinating idea for the debate on the responsibility of intelligent systems. Among the various hypotheses proposed, there is the introduction of a new legal category: the electronic person (or even electronic personality). This is a subject with its own legal status, holder of rights and duties and responsible for the damage caused. This new figure joins those already comprehended in our legal system, to regulate the distinct responsibility for damage caused by

[39] The names of the members can be found on the MiSE website: <mise.gov.it/index.php/it/10-istituzionale/ministero/2038906-intelligenza-artificiale-membri-del-gruppo-di-esperti>.

[40] See <https://www.mise.gov.it/images/stories/documenti/Strategia-Nazionale-Intelligenza-Artificiale-Bozza-Consultazione.pdf>; for an overview of Italy's political initiatives regarding AI see also the OECD website < https://www.oecd.ai/dashboards/countries/Italy>.

robots.[41] This hypothesis includes all those harmful consequences that cannot be predicted during the design phase of the "machine", nor can they be avoided by applying due diligence. However, above all, the recognition of this new legal subjectivity would allow the legislator, through a legal fiction, to solve the problem of the imputability of liability and to better organise risk management. Behind the subjectivity of the robots, an apparatus capable of distributing between the subjects involved in the various phases of creation the AI system, the economical charges deriving from any damage, constituting an "associated asset mass to the machine" which guarantees the damage. Such an asset consists of the same subjects involved in AI who would thus limit the concerns inherent in the danger of the new "machines", returning to invest in the research and production of new technological systems safely. Europe itself is moving in this direction.[42]

If one accepted the idea that an AI system can make autonomous decisions following the acquisition and processing of one's own experience, one could risk extending Art. 2043 of the Italian Civil Code also to this new "subject". It would be equated with a sentient being similar in all respects to human. We can consider that latter thesis rather original, both for jurists and philosophers, but in line with the vision of law open to every new experience and continuous evolution and transition, reaching out towards a posthuman (or transhuman) future, with the task of regulating any new reality.[43]

AI has the "ability to learn and act" based on accumulated experience. Therefore, it cannot be considered as an object, a tool, or an activity. This aspect, since it predisposes the AI systems to become autonomous in the decisions, also makes them "unpredictable" with respect the intentions assigned by the programmer. Therefore, the AI system could cause damage to the human user/user without the intention or active participation of the individual who created it, thus missing the (human) subject to which to attribute the harmful event and the responsibility. There would be no causal link between the conduct/intent of the person who designed (or produced or distributed) the AI and the harmful consequences produced autonomously by the system itself. In order to have a complete discipline, references to other disciplines multiply in the search for other forms of responsibility. As an example, references to the damage caused by minors as subjects "who learn during their growth" are equated for AI systems based on machine learning. This equation would allow the reference to the figure of parental responsibility according to Art. 2048 of the Italian Civil Code considering the programmer as the responsible for the work of his "creature". Another hypothesis could be the responsibility for harmful or dangerous actions under the Art. 2050 of the Civil Code. The most appealing perspective hypothesises the predisposition in sentient AI systems of an ethical code, so that they can recognise

[41] See A. Massolo, 'Robot e responsabilità per danni: basi giuridiche' (19 October 2018) Agenda digitale <https://www.agendadigitale.eu/cultura-digitale/robot-e-responsabilita-per-danni-basi-giuridiche>,

[42] See European Parliament resolution of 16 February 2017 on Civil Law Rules on Robotics, P8_TA(2017)0051; European Commission Staff Working Document, Liability for emerging digital technologies, SWD(2018) 137 final, 25 April 2018.

[43] "Do not take your eyes off these new territories", typical of a law capable of evolving and which is in continuous transition, cf. Rodotà (n. 20).

what is lawful and what is not. Such a code should be included in the AI operating algorithm, providing it with a moral.

Also for criminal law exist the issue of liability for damage caused or connected to the use of intelligent systems both as products and as agent systems and there are the two hypotheses of a not sophisticated AI used to commit a crime and an "agent" AI capable of self-determination. However, there are rigid principles of legality and taxation of the cases and it is challenging to hypothesise that a subject can respond criminally (and therefore can be subjected and sanctioned) "for the autonomous, inevitable and unpredictable conduct" of an AI capable of to self-determine. Furthermore, criminal liability is a personal responsibility as provided for by our Constitution in Art. 27 and this means that no one can be held responsible for a harmful activity carried out by "other" people. The person who committed the crime must be a natural person, defined, in fact, the active subject of the crime[44]. The consequence is that it becomes somewhat hard to predict forms of crimes attributable to non-human subjects, as in the hypothesis of an Intelligent Agent, even if some scholars have still developed "alternative" theories in this regard. Some scholars,[45] for example, states that there are no valid reasons to deny the punishment of an AI, because it may be responsible for its work as it has acted autonomously due to its nature of machine learning. The operator/creator, therefore, could not be held responsible even for negligence, as the robot's action is unpredictable as a result of its data processing activity that allows it to act independently. Nevertheless, the criticisms levelled at this theory are based on the total independence of AI, because the programmer (or operator-producer-or user) must be held responsible for not having foreseen the "dangerous unpredictability" of the system. The effect would take the responsibility for fault, or responsibility that occurs in the hypothesis where "all the consequential links" of the causal process caused the damage/injury are not known.

Overall, the hypothesis now proposed, albeit suggestive, offers an opportunity to reflect on exciting developments in the law, such as the application of direct criminal responsibility of an Intelligent Agent equating it to the figure introduced with Legislative Decree 231/2001 which derogated from the general principle *societas delinquere non potest*. The Decree introduces a sort of direct criminal liability of companies envisaged for some types of crime.

Realistically, the law claims that humans must always be responsible for the work of AI by resorting to liability already provided for in the legal system, namely the responsibility for the production and distribution of potentially dangerous products. In this case the intelligent agents involved, even if autonomous and sophisticated, would be considered the "products" or the "results" of technology. Products and results hard to handle and that entail more significant risks for humans than the benefits, the so-called "Risks of technological innovation". The solution may consist in generating parameters to respect during the creation, production and use of AI products. The cautions could be reduced to the simple consideration of "carefully

[44] Therefore, the so-called cc.dd. Legal entities. In this regard, however, it should be noted that Legislative Decree No. 231 of 2001 makes an exception to the general principle "societas delinquere non potest", introducing a sort of direct criminal liability of companies for certain types of crime.

[45] G. Hallevy, professor of Criminology at the Faculty of Law of the Israeli University Ono Academy College, who also wrote a book on the subject entitled *When robots kill: artificial intelligence under criminal law* (Northeastern University Press 2013).

evaluating the benefits AI to the individual, compare these with the corresponding dangers and decide whether to produce and distribute them or give them up". In practice, a sort of codified common sense that answers the simple questions: "Are the benefits greater? If the answer is yes, production is allowed. Are there too many risks associated with the production? If yes, production is denied.

At present, a more realistic and adequate criminal liability of the inactive operator seems to be envisaged and able to guarantee the presence on the market of an innovative and safe technology. At least for now, it seems wiser to answer negatively the question whether the *machina delinquere potest*, thus resolving also aspect: *quomodo machina punire potest* because It would be questionable to identify the type of punishment more adequate to deliver to a criminal AI.

5. *Conclusions*

We can conclude with a brief consideration on the danger of the new technologies applied to information. Mastering information and accessing quality information places us in a position of power. The information allows us to decide and choose, making the individual difficult to manipulate above all by algorithms. The control must also concern the conscious attitude to online, an environment that radically transformed from a space of absolute freedom, as it originally was, to a dangerous place of "social enticement". The so-called cyberspace or, as defined today, the digital world, is transforming from a place that protected anonymity, freedom of speech and individual control, into a place that makes anonymity increasingly tricky (perhaps this does not look a negative feature), less free speech and individual control tending to concentrate in the hands of a few experts. For a fascinating in-depth analysis, we refer to the reading a short article, entitled "Code Is Law" of Lawrence Lessig[46] published in Harvard Magazine in January 2000[47]. The article highlighted, as far back as 1999, how every era stands out for its "potential regulator ", the regulation that can monitor the activity of the individual in a new context. Lessing claims that in the cyberspace, our regulation is represented by the Code (the software and hardware that characterise cyberspace) and whoever holds it has the power to determine: 1) how and if to protect privacy, 2) how and whether to censor freedom of expression and 3) how and if it is possible to access which information. This allows you to control everything.

Awareness is the main element capable of helping us to control technologies and convince us "that we must not be […] intelligent enough to operate machines and at the same time stupid enough to accept their abuse, rather, there must be machines […] intelligent enough to work but stupid enough to accept their condition». We must create machines that work the best and nothing more. By doing so, our attitude towards AI systems would not be dominated by the fear of a sci-fi and apocalyptic future, where machines will control the humankind. In 2003, Nick Bostrom[48]

[46] Professor of law at Stanford Law School, founder of the Center for internet and society, scholar of copyright rights and free access to information as well as of the strong influence that technology has acquired in the world of information, a true guru of digital and of the network.

[47] See <https://harvardmagazine.com/2000/01/code-is-law-html>.

[48] Philosopher and scholar of the so-called existential risk, professor at the University of Oxford, where he directs the Future of humanity Institute. The brief considerations drawn in this context have been

developed a theory concerning human evolution and the transformation of humans in a slow and gradual hybridization with the machine. If the "machine" prevails over the "human" element, evolution would be destructive for human race. The alternatives to a prevarication of the machine over humans could consist in designing "thinking" machines controllable and provide them with a "suicidal switch", for safety. A switch that can turn the machines off in case of danger; or even design AI aligned with human values, i.e. ethically programmed[49]. A simple button, plus a wealth of ethical values, could save humanity and the transition from *homo sapiens* to transhuman could no longer represent a danger but rather an improvement.

The danger, however, remains hidden behind the fleeting border "between what is most useful to us and what we like most", satisfying our less noble desires. The use of ethics, once again, would represent an anchor of salvation. It is now time to worry about "new technologies before let they take care of us".

extrapolated from a work of his entitled *Superintelligence. Trends, Dangers, Strategies* (Oxford, Oxford University Press 2014).

[49] Both hypotheses are, moreover, already contemplated in the European Union AI Guidelines.

LABOR RELATIONS, INTELLIGENT MACHINE, DIGITAL PLANTS. LEGAL PROBLEM RELATED TO DATA AND SOCIAL PROTECTION

MICHELE FAIOLI

SUMMARY: 1. Outlining the legal issues and the social problem. – 2. Improving workplace regulations by procedures. – 3. The third element of the labor relations. Intelligent Machines exercising employer's powers – 4. Conclusions. Building up a new discipline ("Labor-Robot Law"). Challenges and scenarios.

1. *Outlining the legal issues and the social problem*

A new organizational model is being applied to work, overtaking the classic (and usually divisive) categories through which the phenomenon is analyzed according to the Fordist theory (by way of example, organization – subordination – powers – rights – obligations). Work entails important theoretical questions if it is linked to the most advanced technology (in Europe, in particular, Industry 4.0 and Gig-Economy). If work has already been considered "incomplete" (non-hyphenated word) because a feature of the employment contract under a market economy is its incompleteness,[1] given that work-effort bargain and labor capacity cannot easily be specified ex ante, it should be expected to be all the more "in-complete" in the future due to the peculiar legal relationship that will come to life among (i) the worker, (ii) the employer, and (iii) the machine endowed with artificial intelligence (intelligent machine[2]). The hyphen between "in" and "complete" bears witness to such legal relationship. The intelligent machine can be considered as a third subject, as it is a "third element" that takes part in the legal matters of the contractual pattern involving the employer and the worker. Therefore, beyond traditional scenarios in labor law, there are wider prospects. These prospects concern the impact of the intelligent machine on work organization in the factory of the future. This is probably one of the reasons why labor regulation is changing and will change further. Law and collective bargaining provisions adapt to technology inasmuch as they are shaped by the latter; such provisions do not determine a separated system; labor regulation has instead built (and will build) the most important part of its logical and legal tools on technology. In the close future, the object of the employment contract will necessarily be complemented with the monitoring and

[1] See S. Deakin and E. Zheng, 'Pricing Labour Capacity: The Unexpected Effects of Formalizing Employment Contracts in China' (2016) 479 Centre for Business Research, University of Cambridge Working Papers 1. To define incomplete work, Deakin and Zheng draw on R. H. Coase, 'The Nature of the Firm: Influence' (1988) 4 Journal of Law, Economics, & Organization 33. See also my recent book M. Faioli, *Mansioni e macchina intelligente* (Giappichelli 2018).

[2] The intelligent machine goes beyond the imitation of the human being. See the reasoning by T. Cowen, *Average is Over* (Dutton 2014): "it does something other than imitate or try to imitate a man" (144). Cf. also the remarks by the Executive Office of the President of the USA, Artificial Intelligence, Automation, and the Economy, December 2016 <https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF>.

regulatory action carried out by machines (third element) on those job tasks the worker will not be stripped of by the most advanced systems created by micro-electronics and computers and related to automation of industrial processes, logistics, transportation, data elaboration, accounting, quality and cost monitoring, medical interventions, biological and chemical processes, waste disposal, selection of materials, etc.

My research sets out to provide some answers to the following questions: how is work in a company changing (or has it already changed) in view of the most recent and innovative technological developments, as well as of foreign investments betting on artificial intelligence? How will work labor-regulations change in Europe in the close future, taking into account that automated and smart technology develops at a fast pace in all productive sectors? To what extent and how should EU labor-regulations deal with the fact that intelligent machines (i.e. the third element of the employment contract), endowed with deep learning, will decide, and monitor, patrol, indicate, define, workers' job tasks? Can we empower such intelligent machine with a sort of "labor legal status"?

The intelligent machine can be considered as a third subject, as it is a "third element" that takes part in the legal matters of the contractual pattern involving the employer and the worker. These prospects concern the impact of the intelligent machine on work organization in the factory of the future. This is probably one of the reasons why labor regulation is changing and will change further. Law and collective bargaining provisions adapt to technology inasmuch as they are shaped by the latter; such provisions do not determine a separated system; labor regulation has instead built (and will build) the most important part of its logical and legal tools on technology.[3] "Technology" and "intelligent machine" are used as synonyms in this paper. My research work sets out to consider labor law in dynamic connection with work organization within the firm, reinterpret the relationship between job tasks/professionalism and the new technological or artificial intelligence systems (organized/integrated economic activities). This issue is particularly interesting, also due to its methodological aspects. An unprecedented transformation in terms of technology and work organization is currently going on. We are going beyond the industrial revolution and Fordism. A new business model is being applied to work, overtaking the classic (and usually divisive) categories through which the phenomenon is analyzed according to the Fordist theory (by way of example, organization – subordination – powers – rights – obligations). Work entails important theoretical questions if it is linked to the most advanced technology. It is impossible to contrast the change in, or the adaptation of, corporate organization, which is strongly affected by competition, international trade, spreading of smart models for HR management, smart technology and hi-tech systems, drone technology, and advanced research hubs. To sum up, that company is a "smart factory".

The rupture in the Fordist paradigm, which – according to some scholars – has not been fully perceived yet,[4] is going to impact, with all its strength, also on those sectors that are more reluctant to experience changes. It should be noted that there is a sort of

[3] In this regard, cf. the remarks by G. Vardaro, 'Tecnica, tecnologia e ideologia della tecnica nel diritto del lavoro' (1986) 1 Politica del diritto 75 and by G. Giugni, 'Il processo tecnologico e la contrattazione collettiva', in F. Momigliano (ed.), *Lavoratori e sindacati di fronte alle trasformazioni del processo produttivo* (Feltrinelli 1962).

[4] L. Pero, 'Come cambia il lavoro di fabbrica. Tecnologie, globalizzazione e intelligenza collettiva' (2013) 46 La società degli individui 30.

suspicion arising from the industrial relations systems. Unlike in the legal systems of other EU countries, in the Italian legal system regulation has focused on forms of flexibility to be applied when entering (types of contract) or leaving (remedies in case of dismissal) the labor market; however, regulation has not dealt with forms of flexibility within the employment contract, which include the worker's in-company mobility. The latter underlies the possibility to change (unilaterally or consensually) job tasks in relation to a specific classification system/pay scale structure. The Italian case law has offered different interpretations of in-company mobility.[5]

2. *Improving workplace regulations by procedures*

We can thus become aware of the existence of a problem underlying all the other issues, which has been outlined in case law: can collective bargaining encounter limitations in this specific area of protection? What kind of professionalism are we seeking protection for before the court in the case of the worker with a specific job task, compared with the one who is tasked with mail delivery, if professional mobility has been confirmed in the collective bargaining contract, including in the firm-level one?

The questions referred to in the previous paragraph show that Art. 2103 of the Italian Civil Code, before the 2015 reform, was definitely inadequate with regard to the rupture in the Fordist paradigm. In many respects, the same provision was inadequate also with regard to Fordism.[6] Unlike other legal systems, in the Italian one it has not been possible to introduce a firm-level procedure, to be authorized by law, that allows the employer, in cooperation with employee representatives, to take measures (also with divesture if justified by objective reasons) that have a substantial impact on individual positions. The choice made by some legal systems (in particular, France and Germany) is underpinned by the idea that the worker's mobility does not fall under civil law, nor is it an issue to be fully regulated through NCBAs. It should rather be dealt with at firm level, in compliance with a specific procedure involving agents authorized to exercise rights and powers in the interest of the working community. In more proactive terms, the NCBA, which is tasked by the legislator with setting out and periodically updating classification systems, is supposed to establish the procedure (taking into account the sector, firm size, and other specificities) as well as to monitor compliance within the firm through the use of paritarian institutes. In a corporate context, instead, economic, individual, and collective interests appear to be intertwined, balanced, and reconciled in the procedure involving the employer and workers' representatives. Following the 2015 reform, the Italian regime has been modified, bearing in mind the scenarios that had long been "envisioned" (cf. the report prepared by the *Consiglio Nazionale dell'Economia e del Lavoro* (CNEL)[7] in 1985 and the Agreement on Productivity signed

[5] In this regard, cf. A. Occhino, 'La clausola collettiva di fungibilità tra mansioni contrattualmente, ma non legalmente, equivalenti è valida per esigenze aziendali temporanee' (2007) 2 Rivista Italiana di Diritto del Lavoro 336.

[6] F. Liso, *La mobilità del lavoratore in azienda: il quadro legale* (Franco Angeli 1982).

[7] As to the "expected" reforms of Article 2103 of the Italian Civil Code, see the CNEL Report "Osservazioni e proposte sulla revisione della legislazione sul rapporto di lavoro", Assembly No. 206 held on 4 June 1985, and F. Liso, 'Brevi osservazioni sulla revisione della disciplina delle mansioni contenuta nel decreto legislativo n. 81/2015 e su alcune recenti tendenze di politica legislativa in materia di rapporto di lavoro' (2015) 257 WP C.S.D.L.E. «Massimo D'Antona».IT 1. See also T. Treu (ed.), *Statuto dei lavoratori e futuro delle relazioni di lavoro* (CNEL 2020).

in November 2012). It was clear why the court has been asked by the parties to an individual employment contract to interpret the concept of equivalence of job tasks and why trade unions and employers' organizations have partly refrained from regulating the phenomenon, failing to adapt classification systems to the new organizational and technological structures. Under the previous regime (1970-2015), the court was asked to interpret the concept of equivalence of job tasks and create significant consequences on corporate organization. This is why the worker's professionalism has been identified as a limitation on the exercise, by the employer, of managerial powers and of the right to modify the work conditions without employees' consent (*jus variandi*). In the aftermath of the 2015 reform, given the new functions that the law assigns the collective bargaining, the professionalism of the worker will not be less protected. Further, in the aftermath of the 2015 reform, the professionalism of the worker will be likely to receive more protection by means of the collective bargaining in relation to the internal (corporate) market or the external (inter-company) market. The new functions and scope of collective bargaining in the framework of the 2015 amended Art. 2103 of the Italian Civil Code are related to each and every corporate context. The focus is on the collective bargaining and firm-level unilateral regulation that have set rules on job tasks, and in particular, the clauses defining modalities of internal flexibility concerning the pay scale structure, job tasks, versatility, and wage are outlined (SMEs and European, Asian, and US multinationals, emphasizing the impact of corporations, private equity funds, and foreign direct investments on work organization and job tasks). There exists a certain ability of collective bargaining (or of firm-level internal regulations) to anticipate needs and to tackle problems, even beyond applicable legislation.

3. *The third element of the labor relations. Intelligent Machines exercising employer's powers*

But this is not enough. In the close future, the object of the employment contract will necessarily be complemented with the monitoring and regulatory action carried out by intelligent machines, or here also "robots", on those job tasks the worker will not be stripped of by the most advanced systems created by micro-electronics and computers and related to automation of industrial processes, logistics, transportation, data elaboration, accounting, quality and cost monitoring, medical interventions, biological and chemical processes, waste disposal, selection of materials, etc. We will access that "deep learning software" technological phase through which the machine is enabled to make sense of the language, create connections, and interact as human beings usually do. In this sense, today workers can still "avoid" that some activities are carried out by machines because the former decide what the latter can or cannot do; in the close future, instead, intelligent machines, which are endowed with deep learning, will decide whether and to what extent they will "strip" workers of their job tasks. The technological development process appears to be irreversible. Ever-more advanced research and the fact that costs are becoming day by day more affordable, also by SMEs, show that the process has already been marked out.

It is a process that goes beyond Post-Fordism. It is the machine that teaches itself what to do, how to do it, and which outcome(s) should be achieved, coordinating human beings, too. The evolution of the object of the employment contract will be determined by the relationship between, on the one hand, the job tasks still performed by human beings and, on the other, those ones human beings have been stripped of by automated and computerized machines that monitor/manage processes in their entirety. All of this will lead to the reorganization of classification systems or pay scale structures, as well as of hierarchies (more or less pyramidal in nature) and the procedures for the assignment of tasks and roles. Workers will be required to carry out more flexible tasks featuring the already known phenomena of job enrichment (determinable job tasks) and job enlargement (modified job tasks). The replacement of workers in those tasks will also be determined by organizational models applied at firm level for the production or provision of the service, including in subcontracting chains (drive system of management – DSM, scientific management – SM, lean production – LP, quality-focused involvement – QFI, teamwork production systems – TPS, modular production – MP, and acceleuction). Such organizational models will impact on the object of the employment contract; as a consequence, they will be translated into specific contents of job tasks, in addition to affecting working time management, pay, staff training, etc.

The incidence on the employment contract means: (i) integration of work organization with the firm-level technological model; (ii) integration between technological procedures and HR management; and (iii) integration between workers' training and job tasks. If we focus on these three items, we can see that the company premises are defined by technological, automated, and computerized innovations. This vision translates into the fact that a shift is taking place from the (geographically identifiable) production unit to the global supply chain, in which several, virtually unlimited, production units – which are based on one of the organizational models referred to above – are connected. In this way, the wall-to-wall dimension of the company unit at global level is enlarged, and a new relationship with clients, suppliers, markets, etc. is established.

4. *Conclusions. Building up a new discipline ("Labor-Robot Law"). Challenges and scenarios.*

Within such a complex framework, a worker (or group of workers) with specific job tasks and covered by a specific employment contract, including a specific classification system stemming from national collective bargaining, is concerned by a wealth of automated and computerized technology innovations, which impact on them as an individual and require specific knowledge (through the replacement of workers by machines, as said above) and probably coordination with other workers (in the same workplace or somewhere else). This does not hold true only for the most advanced types of professionalism. Instead, the opposite is true, based on the close observation of some significant companies in sectors deemed to be strategic for the Italian economy. Such technological evolution also determines the transformation of job tasks and classification systems. This demonstrates that the classification systems envisaged in NCBAs are outdated. Almost all the NCBAs have regulated (and continue to regulate in their renewed versions) staff classification systems, taking into account mere operational activities that are simple, repetitive, and classifiable. Consequently, job tasks, too, were/are intended as tasks – inseparable basic units – that are assigned to the worker in the framework of a specific business organization. It follows that the job task is still considered as a combination of phases, operations, and elementary movements.[8] Those classification systems are not based on models aimed at the coordination, management, and monitoring of results from the combination involving the worker, the working team, and automated technology, the latter being responsible for stripping workers of their assignments, functions, and activities, shortly of their job tasks.

It follows from the above that there exists a new setting of job tasks in an industrial world that changes owing to bio-inspired automation, artificial intelligence, and the most technologically advanced organizational models (the so called "CO-BOT"). Such legal setting is shaped by this technology.[9] Inasmuch as the provision in force prior to the 2015 reform was inadequate with regard to the evolving reality, the theory of job tasks does no longer properly tackle the issues raised by technology. A (new) theory of job tasks must, instead, shift to the idea that – through a specific procedure – rights, too, can be balanced against situations that may affect the exercise of the right to work. The (new) theory should deal with the entitlement itself: could workers' representatives in the company be deemed to be entitled to enjoy those rights? If so, could the exercise of that entitlement be proceduralized? The (new) theory should acknowledge the existing limitations on the exercise of the power of divesture in the framework of collective bargaining.

From this perspective, the goal of my research is to propose a methodology aimed at outlining a theory of job tasks in a changing industrial world under pressure from the intelligent machine, which teaches itself, "coordinates" the working activities of human beings, and strips workers of their job tasks. Over time, the picture will become more complex as company-related events will be measured, thus generating huge quantities of archived data (big data); such data will furthermore be analyzed by systems aimed at supporting decision making and based on artificial intelligence technology (cognitive systems). It should be added that there will be the possibility to communicate such data with real-time remote control from one end of the world to the other; as a result, employers' powers, business networks, and even the notion of "employer" will be reshaped.[10] This is a new theory of job tasks, here also defined "Labor Robot Law", in the factory managed by artificial intelligence (third element of the employment contract): the relationship between the intelligent machine, representing a sort of third element of the contract, and the employer's powers should be more precisely investigated. Such third element is key to understand the legal issues relating to the compatibility between job tasks, staff classification, and the most innovative organizational models (acceluction, lean production, team working, etc.), which are included into the organizational processes that are directly coordinated by machines endowed with artificial intelligence.

We have at least two forthcoming scenarios. The first is related to the short-middle term. The secondo may occur somewhere in the longer term. Both scenarios are based on the idea that legislation is just one of the regulatory instruments: we should have and

[8] If we read once more the classics in relation to this issue, we get the impression that, as early as during the Italian economic boom, there were some doubts on this vision. We can feel the change already in G. Giugni, *Mansioni e qualifica nel rapporto di lavoro* (Jovene 1963).

[9] To define some technological innovations that will impact on the organisational model of the factory of the future, Camera dei Deputati, Commissione X, *Indagine conoscitiva su "Industria 4.0"*, 2016.

[10] See the 2019/2020 invetigations on artificial intelligence of the Italian Government <https://www.mise.gov.it/index.php/it/intelligenza-artificiale-call>.

promote a balanced mix of law, collective bargaining norms, market and technology in order to determine better outputs than just black letter law can offer.

Firstly, regulating artificial intelligence or robots at workplace level does not means regulating artificial intelligence/robots themselves or having them as the target of regulatory intervention (at least until a legal capacity of artificial intelligence/robots is defined by law). Regulating artificial intelligence or robots at workplace level implies that collective bargaining, within a frame that should be fixed by law, pursues the aim to allow a fair interaction between workers and robots. Hence, labor robotics regulation is a more accurate term to indicate an academic field we are proposing in this investigation: such regulation is aimed at influencing the behavior of workers in the context of robotics application and developments at firm level.

The second scenario is more complex to explain, but very useful for the conclusions. In the case, somewhere, in the longer term, artificial intelligent would be considered as legal subject acting at firm/plants level, labor regulation should build part of logical and legal tools on advanced technology, robots, smart factory, etc.. The dilemma is that regulators cannot intervene too early, nor too late.[11] EU/States labor-regulations should deal with the fact that intelligent machines will improve its own ability to decide, and monitor, patrol, indicate, organize, define, workers' job tasks. If we empower such intelligent machine with a sort of "labor legal status", we should also empower collective bargaining for facing with intelligent machines because we need a context-specificity regulatory approach. Robots, that differ in many features, must be addressed at concrete levels in their own contexts. Collective bargaining, at firm level, is therefore the best way to regulate such phenomenon. Regulation must be dynamic, cyclic, interactive and a mean to involve unions and employers. Empowering such collective bargaining will determine that not the technology, but rather the adverse effects at firm level of artificial intelligence should be regulated by unions and employer, within a general legal frame and by means of procedures. The law could be inadequate to cope with robots' adverse effects at firm level, while collective bargaining could more precisely regulate such adverse effects, and, consequently, vary in time and place and be more or less flexible, in relation to the firm and the production, the research in technology and the application at firm level.

This proposal is based on the fact that if legal regimes can be adapted in relation to the substantive challenges, regulators must exercise forms of awareness of "challenges at a deeper level of the law" [because] Robotics […] challenge assumptions underlying regulatory frameworks as a whole, such as the distinction between things and humans [...] This requires careful reflection on what regulation aims to achieve, when society slowly but inexorably changes shape through fundamental socio-technical changes".[12]

[11] D. Collingridge, *The Social Control of Technology*, St Martin's Press, 1980.

[12] E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini and F. Lucivero, 'Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues' (2017) 9 Law, Innovation and Technology 1.

PART II

USE OF UNMANNED AERIAL, MARITIME AND GROUND SYSTEMS IN CIVIL AND MILITARY FIELDS

INTRODUCTION

STEFANO POLLASTRELLI

Since the last two centuries innovation technology has always presented challenges for the humans being in the field of transportation. The use of steam as propulsion has changed the relation between people and geography opening the window for an era that has commonly recognised as the origin of the modern globalization. After the Second World War we have also discovered the impact of the aviation on private and commercial behaviour filled the gap in the framework of a globalized world. Information technology and electronics have helped but until a couple of decades ago the main drivers of mobility and transportation were those past invention performed and implemented to match the needs of post-modern era. This framework is going to be changed or, to be correct, it has already changed. In this sense automation and digitalization are bringing us in a new era, again!

Looking at aviation and air traffic control services the recent proposal of the implementation of the Single European Sky (SES2+) is grounded on a heavy use of technology aiming to overcome the current (and ancient?) picture of the national airspace and designed a common EU airspace. The outcome of this approach should be more efficiency – in terms of flight environmental sustainability and cos saving – as well as enhance of safety. In this sense the use of trajectory-based-operations (TBOs) for aircraft navigation needs to be helped by the support of satellite air traffic control system able to achieve the goal of augmented air traffic control situation awareness. As S. Magnosi in his contribution highlights this kind of technology points out some needs in terms of regulation and legislation as well from liability perspectives to international law ones, calling also for the involving in this process users and operators in order to balance risks and opportunities.

The same awareness arises from the C. Telesca paper related to road transport and automation. Moving its first steps into the aviation field, the automation has recently extended its range to the road mobility and transportation. The ultimate goal of a driverless car is not far to reach due to the fact that carmakers have already implemented some automated technologies in order to enhance safety with clear positive results. But as the Author points out this kind of revolution requires a broad approach involving not only the regulation in relation to liability for consumers and users. Indeed, the impact of the driverless car is wide and calls for the rethinking of infrastructure – that should be able to "communicate" with autonomous vehicle – manufactures, insurance, hardware and software designer in order to get a fair apportionment of the risks and allowing benefits for the consumers.

Also moving towards the maritime law, the innovation technology undermines the long and strong commercial practices across the world. The invention and above all the practical capability of unmanned vessels should be firstly addressed from the definition in order to apply all international conventions that rule the international maritime trade and shipping as well. In this sense the contribution by A. Caligiuri makes clear all the uncertainties and difficulties to address these issues, to reach the uniformity and harmonization among all international maritime legal instruments, also highlighting the amplification of these questions once the discussion shifts towards military application.

Concerns are then pointed out in the paper from A. Amoroso and G. Tamburrini in relation to the combination of automation and lethal weapons. From this perspective questions about legal aspects are accompanied by ethics ones. Issues like the responsibility about the use of autonomous weapons (AW) and their relationship with the "human control" alongside the concern over the human dignity are far to have clear answers. And recent events – as the Nagorno-Karabakh war in November 2020 in which AW have made the difference – also remember us the necessity to move the question from a legal to a political and geopolitical point of view.

Definitely the constant innovation technology is painting a picture in which *disruptions* are the "new normal", in which the response by rulemakers is slow and often unfit to rule its civil and military application. Machine learning, artificial intelligence that are the grounds of automation, highlight huge problems in terms of responsibility, liability and apportionment of the risk as well as ethical one. The way forward for the jurist is to understand the innovation that are far from the older ones and far for traditional training and that are calling for the necessity to be ruled and regulated otherwise legal and ethical issues are remain unfulfilled and tending to amplify.

AIR TRAFFIC CONTROL BY SATELLITE: SOME LEGAL ASPECTS

SILVIO MAGNOSI

SUMMARY: 1. Origins and Evolution of the Air Traffic Services. – 2. The Use of Satellite Navigation Systems in Air Traffic Control. – 3. European Union and Satellite Navigation Systems: The GALILEO Project. – 4. Liability Issues. – 5. Satellite Navigation Systems and International Space Law.

1. *Origins and Evolution of the Air Traffic Services*

Air navigation has always been regulated by specific and codified international law. Someone has seen, in this particular element, a difference between air law and maritime law, even within a unified and autonomous regulatory system, such as the Italian navigation law. In other words, it has been noted that international maritime law is based on the practice of trade. This practice has spread and been consolidated over the years and it has finally been codified in international conventions. On the other hand, air law has been based, since its origins, on international conventions; even if they used legal principles, similar to those operating in maritime navigation.[1]

The Paris Convention 1919[2] was the first real international treaty governing civil aviation and air navigation. Everyone can note that we are at the dawn of air transport. At that time, the aviation industry received an important increase from the large use of aircrafts, during the World War I. The Paris Convention had a limited diffusion, but it was very relevant because it affirmed the fundamental rules of international air law. Some years later, many of these rules and principles were incorporated into the Chicago Convention 1944 on International Civil Aviation.[3] We

[1] For a specific analysis of differences and affinities between air and maritime law, cf. from various points of view, A. Lefebvre d'Ovidio, 'La pretesa autonomia della parte aeronautica del codice della navigazione' (1942) Rivista di diritto della navigazione 321; E. Spasiano, 'Oggetto limiti ed integrazione del diritto della navigazione' (1961) Rivista di diritto della navigazione 43; E. Spasiano, 'Il diritto della navigazione come sistema unitario ed autonomo' (1963) Rivista di diritto della navigazione 279; M. Grigoli, 'L'unitarietà del diritto della navigazione' (1973) Il Diritto aereo 7; S. M. Carbone, 'La cosiddetta autonomia del diritto della navigazione: risultati e prospettive' (1975) Il Diritto marittimo 24; G. Romanelli, 'Diritto aereo, diritto della navigazione e diritto dei trasporti' (1975) Rivista trimestrale di diritto civilr 1331; G. Rinaldi Baccelli, *Studi di diritto aeronautico* (Giuffrè 1977) 4 ff.; T. Ballarino and S. Busti, *Diritto aeronautico e spaziale* (Giuffrè 1988), 16 ff.; G. Pescatore, 'Diritto della navigazione e principi generali', in *Studi in onore di Gustavo Romanelli* (Giuffrè 1997) 971 ff.; S. Piazza, R. Borile and R. Fettarappa, *Diritto della navigazione aerea* (Zanichelli 2000), 4 ff.

[2] *Convention de Paris de 1919 portant réglementation de la navigation aérienne.* Cf. S. Cacopardo, 'La Conferenza di Parigi sul diritto privato aeronautico' (1925) Il Diritto aeronautico 36; A. Giannini, 'La Convenzione di Parigi per il regolamento della navigazione aerea', in *Saggi di diritto aeronautico* (Vita e Pensiero 1932) 23 ff.; E. Turco Bulgherini, *La disciplina giuridica degli accordi aerei bilaterali* (CEDAM 1984), 7; Ballarino and Busti (n 1), 51 ff.; U. Leanza, *Il diritto degli spazi internazionali*, *I - La tradizione* (Giappichelli 1999), 354.

[3] International Civil Aviation Conference Convention on International Civil Aviation, signed at Chicago, 7 December 1944 and entered into force on 4 April 1947. See A. Giannini, 'La Convenzione

can recall the rule that establishes the complete and exclusive sovereignty of every State over the air space above its territory,[4] its territorial waters and extraterritorial regions. We can also remember the establishment of an international organization, capable of adopting technical and uniform rules on air navigation: the old CINA – *Conference internationale de la navigation aérienne* – in the Paris Convention and the modern ICAO – International Civil Aviation Organization – in the Chicago Convention.[5]

The first international rules on air traffic services can be found in the Paris Convention itself. These services are necessary tools for safety and efficiency of air navigation and were established together with civil aviation. This is another difference between air and maritime navigation. Indeed, the ship commander has always been the only protagonist during the navigation (*après Dieu, le capitaine*). Some external navigation aids have only recently been introduced. On the other hand, Art. 25 of the Paris Convention 1919 established the duty to observe the rules of Annex D for every aircraft registered in the Contracting States. Among the Paris Convention Annexes, Annex D was the only one containing imperative provisions. Its rules concerned air traffic in general: air navigation procedures, rules of the air, measures to fly over airport areas, landing and take – off procedures, surface signals such as lights, flags etc.[6]

Since the end of the World War II air transport has had a great development. Air transport was no longer an exclusive mode of travel, but progressively became a new form of mass transportation. Air traffic services consequently followed this large development too. Several rules concerning not only technical and operational profiles, but also legal aspects have been adopted over the years. Thus, the air traffic services were no longer aimed only to protect the navigation safety, but also to guarantee the air transport efficiency and economy.

In this perspective, we can note that the Chicago Convention contains a much more complex and articulated regulatory framework, governing air traffic services. In particular, Chapter IV of the Chicago Convention is specifically and expressly dedicated to the *Measures to Facilitate Air Navigation*. We must also remember Annex

di Chicago (1944) sull'aviazione civile internazionale' (1946) Rivista di diritto commerciale 43; A. Giannini, *La Convenzione di Chicago del 1944 sull'aviazione civile internazionale* (Associazione Culturale Aeronautica 1953); A. Catti, 'Le norme relative alla circolazione aerea (Raffronto tra la Convenzione di Parigi del 13 ottobre 1919 e la Convenzione di Chicago del 7 dicembre 1944)' (1948) Rivista aeronautica 331; Ballarino and Busti (n 1), 56 ff.

[4] According to Art. 2 of the Chicago Convention 1944: "For the purposes of this Convention the territory of a State shall be deemed to be land areas and territorial waters adjacent there to under the sovereignty, suzerainty, protection or mandate of such State". Cf. R. Monaco, 'La disciplina giuridica internazionale dell'aviazione civile' (1956) Rivista del diritto della navigazione 99; Leanza, (n 2), 343 ff.; A. Lefebvre d'Ovidio, G. Pescatore and L. Tullio, *Manuale di diritto della navigazione* (Giuffrè 2019), 99 ff.

[5] Relating to CINA's competences and activities, see S. Cacopardo, 'Navigazione aerea', in *Novissimo Digesto italiano* (vol. 11, UTET 1965) 113-115; about ICAO, F. Lattanzi, 'Organizzazione dell'aviazione civile internazionale (ICAO)', in *Enciclopedia del diritto* (vol. 31, Giuffrè 1981) 228 ff.; Ballarino and Busti (n 1), 83 ff.; A. Sciolla Lagrange, "Organizzazione dell'aviazione civile internazionale (OACI)" in *Enciclopedia giuridica* (vol. 20, Treccani 1990) 1 ff.; A. Masutti, *Il diritto aeronautico. Lezioni, casi, materiali* (Giappichelli 2004), 31-35.

[6] M.M. Comenale Pinto, *L'assistenza al volo. Evoluzione; problemi attuali; prospettive* (CEDAM 1999), 13 ff.

XI of the same Treaty, concerning the *Air Traffic Services*.[7] Furthermore Articles 691 and 691 *bis* of the Italian Navigation Code concern the air traffic services too, and they transpose the provisions of the Chicago Convention, mentioned above.[8]

Therefore, air navigation services are called to meet new and pressing needs, due to the great increase of air transport. On one hand there is the need to continue to ensure and, indeed, to upgrade adequate levels of safety. On the other air transport must result maximally efficient and economically advantageous. To this end, the number and frequency of flights and the number of passengers is certainly important, but the more specifically commercial and financial aspects, linked to market systems, also have some relevance for the development in this sector.

2. *The Use of Satellite Navigation Systems in Air Traffic Control*

Since the early 80s the ICAO has indicated satellite technology to improve air navigation. To this end, the ICAO Assembly established the FANS (*Future Air Navigation Systems*) Committee in 1983, which was followed by the FANS II (*Special Committee for the Monitoring Coordination of Development and Transition Planning for the Future Air Navigation Systems*) Committee some years later. The Committees completed their study and planning activity in 1993.[9] Satellite technology was considered as the only one capable of controlling air traffic in very large areas (for example desert zones or open seas) and capable of allowing precise data communications (meteorological conditions, route and other flight indications etc.). In addition, satellite navigation systems can interact with a wide range of aircrafts and

[7] Para. 2.2 of the Annex 11 to the Chicago Convention points out that: "Air Traffic Services shall be to: a) prevent collisions between aircraft; b) prevent collisions between aircraft on the manoeuvring area and obstructions on that area; c) expedite and maintain an orderly flow of air traffic; d) provide advice and information useful for the safe and efficient conduct of flight; e) notify appropriate organizations regarding aircraft in need of search and rescue aid, and assist such organizations as required". For more specific informations, cf. M. Grigoli, *Il problema della sicurezza nella sfera nautica* II (Giuffrè 1990), 661; M. Grigoli, *Profili normativi della navigazione aerea* (Cacucci Editore 2008), 35 ff.; Comenale Pinto (n 6), 22 ff.; M. M. Comenale Pinto, 'Organizzazione e responsabilità nei servizi di traffico aereo' (2004) Diritto dei trasporti 42; M. P. Rizzo, *La gestione del traffico aereo in Europa tra competenze di enti internazionali e prerogative statali* (Cust 2004), 12; S. Busti, 'Uso dello spazio aereo ed assistenza al volo nella Convenzione di Chicago e negli Annessi e Procedure ICAO', in M. P. Rizzo (ed.), *La gestione del traffico aereo: profili di diritto internazionale, comunitario ed interno* (Giuffrè 2009) 59 ff.

[8] Part II (entitled "Della navigazione aerea") of the Italian Navigation Code was completely revised some years ago. Articles 691 and 691 *bis* were introduced by Legislative Decree No. 96/2005 and amended by Legislative Decree No. 151/2006. Art. 691 identifies and defines air traffic services, substantially transposing para. 2.2 of Annex 11 of the Chicago Convention (n 7). For observations on the revision of Part II of the Italian Navigation Code, cf. G. Rinaldi Baccelli, 'Il progetto di riforma della parte aeronautica del codice della navigazione', in *Il nuovo diritto aeronautico. In ricordo di Gabriele Silingardi* (Giuffrè 2002) 3 ff.; G. Mastrandrea and L. Tullio, 'Il compimento della revisione della parte aeronautica del codice della navigazione' (2006) Il diritto marittimo 699; L. Tullio, 'Codice della navigazione (riforma del)', in *Enciclopedia giuridica* (vol. 6, Treccani 2006) 1 ff.; E. Turco Bulgherini, 'La riforma del codice della navigazione – parte aerea' (2006) Nuove leggi civili commentate 1341.

[9] W. Guldimann, S. Kaiser, *Future Air Navigation Systems. Legal and Institutional Aspects* (Kluwer 1993), 15 ff.; A. Kotaite, 'ICAO Ushers in a Revolution in Global Navigation Technology' (1994) XIX Annals of Air and Space Law 341.

can reduce vertical and horizontal separations. In this way, air space certainly results safer and it can be used according to optimal principles of efficiency and economy[10].

Over the past few decades, satellite navigation systems have received a very large use. Their utilization today involves not only air transport, but all the various forms of transportation. Numerous other sectors are equally involved, such as telecommunication services, agriculture, meteorology. We can say that satellite technology is today an important element of our daily life. For this reason, we are called to examine the legal issues, in relation to the use and applications of satellite navigation systems.

Air traffic services have been always linked to the aforementioned principle of State sovereignty over the airspace above the national territory. Art. 28 of the Chicago Convention 1944 contains an application of this principle. According to Art. 28, each Contracting State undertakes to implement in its territory all the instruments and measures to aid air navigation. This means that each State Party of the Convention must ensure safe and efficient air navigation in the same areas on which it exercises its full and exclusive sovereignty. We can say that, in essence, Articles 1 and 28 of the Chicago Convention represents "two sides of the same coin". The use of new air navigation systems leads to certain changes in the original regulatory framework governing air traffic services. More specifically, the satellite component leads air traffic control activity to the crossing of traditional national borders.

In this regard, the Charter on the Rights and Obligations of States relating to GNSS (Global Navigation Satellite Systems) Services can be appropriately recalled. This document was adopted by the ICAO Assembly in 1998. Although the Charter contains only programmatic provisions, not having binding character, it is however very significant, because it lays down some basic guidelines for the implementation of new air traffic services. Paragraph 3 of the Charter prescribes that satellite navigation systems cannot infringe the fundamental principles of International Civil Aviation (first of all the sovereignty of each State on its respective airspace). At the same time, this provision states that satellite technology can be fully efficient only from a global perspective. In other words, satellite navigation systems have a global dimension, and therefore their use on a planetary and non-discriminatory basis must be guaranteed.[11]

This issue arises in a particular way because there are numerous satellite navigation systems, owned by different States and operated by various national authorities. In addition, we cannot forget that these systems were, in most cases, originally planned and implemented for military purposes, even if they are accessible to all users today. Among several GNSS systems currently in operation, we must mention the "older" US GPS (Global Positioning System, also named NAVSTAR/GPS) and Russian GLONASS (Global Navigation Orbiting Overlay Service) and the "younger" Chinese

[10] A. Cocca, 'The Chicago Convention and Technological Development in Air and Space' (1994) XIX Annals of Air and Space Law 315; J. Huang, *Aviation Safety through the Rule of Law. ICAO's Mechanisms and Practices* (Kluwer 2009); L. J. Smith, 'Legal Aspects of Satellite Navigation', in F. Von Der Dunk and F. Tronchetti, (eds.) *Handbook of Space Law* (Elgar 2015) 604 ff.

[11] The Charter is contained in the ICAO Assembly Resolution A-32/1998. Para. 3 states as follows: "The implementation and operation of GNSS shall neither infringe nor impose restrictions upon State's sovereignty, authority or responsibility in the control of air navigation and the promulgation and enforcement of safety regulations". Cf. S. Magnosi, *Controllo satellitare del traffico aereo e regime di responsabilità* (Aracne 2008), 74 ff.; Smith (n 10) 604.

BEIDOU/COMPASS and EU GALILEO.[12] There are also a lot of both ground-based and satellite augmentation systems, which increase the accuracy and availability of primary satellite constellations. From a legal point of view, this situation gives rise to some problems of compatibility between the traditional needs and competences of the States and the global character of the new satellite navigation technologies.

The adoption of uniform rules which, at the same time, do not infringe the various State competences could be the right way to follow. In such perspective, the Chicago Convention represents an example. As said above, Art. 1 of the Convention establishes State sovereignty on the airspace above the national territory. We have seen also that Art. 28 is a sort of specification of this principle, because it assigns to each State the task of implementing and operating air navigation facilities in its territory. But the Treaty itself contains several provisions which point out a close cooperation between the Contracting Parties. This happens by means numerous uniform rules concerning technical and operational profiles of air navigation and air traffic services. Chapter VI of the Convention is significantly entitled: "International Standards and Recommended Practices". In particular, according to Art. 37, the Parties undertake "to collaborate in securing the highest degree of uniformity" in regulations, development and improvement of the aeronautical sector. We know very well that ICAO's role in this context is essential. The Organization is called to adopt and amend from time to time, as may be necessary, international standards and procedures, dealing with "communication systems and air navigation aids" and "rules of the air and air traffic control practices" among other matters. These standards and procedures are necessarily included in uniform provisions and they must be transposed and applied in the various national legal systems.[13]

3. *European Union and Satellite Navigation Systems: The GALILEO Project*

The European Union has followed the way of uniform regulation in the use of the so called Single European Sky. The European Parliament and Council Regulations (EC) Nos. 549/2004 to 552/2004 ensure that a single air space is established and identified above the territory of the Member States. Such space cannot be certainly regarded as a geographically unified area, but it must be considered only from a functional point of view. In this perspective, Member States are called to adopt and observe uniform rules and principles to guarantee safe and efficient air traffic services in this zone.[14]

[12] Smith (n 10), 556-577.

[13] See above (n 5 and 10).

[14] Cf. Regulation (EC) No. 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation); Regulation (EC) No. 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation); Regulation (EC) No. 551/2004 of the European Parliament and of the Council of 10 March 2004 on the organisation and use of the airspace in the single European sky (the airspace Regulation); Regulation (EC) No. 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation). For a specific and extensive analysis see Rizzo (n 7), 15 ff.; M. P. Rizzo, 'Il pacchetto di regolamenti comunitari per la realizzazione del Cielo Unico Europeo', in *Studi in memoria di Elio Fanara* (Vol. I, Giuffrè 2006) 57 ff.; M. Grigoli, *Aspetti evolutivi del regime nautico. II - La navigazione aerea* (Libreria

The implementation of the GALILEO Project can also be seen as a form of crossing traditional national borders in air traffic control.[15] In this regard, we must remember the European Parliament and Council Regulation (EU) No. 1285/2013. As well known, this Act specifies the different phases of planning and implementation of the Program and points out that the European Union will finance it in its entirety.[16]

Furthermore, Annex D to the Regulation (EU) No. 1285/2013 contains a Joint Declaration by the European Parliament, the Council, and the European Commission, on the establishment of the Galileo Interinstitutional Panel (GIP). The Panel aims to facilitate implementation and operation of the GALILEO Project and all European satellite navigation systems in general. Thus, new satellite navigation technologies address air traffic services towards an international dimension or a supranational and interinstitutional framework.

4. *Liability Issues*

The global dimension of new air traffic services concerns not only technical and operational profiles, but also regards legal and regulatory aspects. Liability arising from satellite navigation systems is surely one of the most relevant issue. This is a very complex problem and hard to solve, because today there arere not specific applicable rules. In addition, numerous and different actors are involved: States, international and supranational organizations, public authorities, private entities. Indeed, the need to adopt an international convention governing liability of air traffic control bodies has been repeatedly stressed over the years. This need seems now more evident, due to the utilization of satellite technologies. In the civil aviation sector some

Bonomo Editrice 2005) 3 ff.; Grigoli (n 7) 46 ff.; E. Turco Bulgherini, *La riforma del codice della navigazione – parte aerea* cit. 1346; R. van Dam and S. Andries*, A Global Single Sky? Some Observations on the Relations between the European Community and International Law in Air Traffic Management* in Annals of Air and Space Law (2006) XXXI 108 ff.; G. Camarda, 'Le imprese di trasporto aereo nell'ordinamento dei servizi aerei' (2007) Diritto dei trasporti 1; S. Magnosi, 'Qualche riflessione sull'impiego della tecnologia satellitare nel controllo della circolazione aerea', in M. P. Rizzo (ed.), *La gestione del traffico aereo: profili di diritto internazionale, comunitario ed interno* (Giuffrè 2009) 299 ff.; S. Magnosi,' Assistenza al volo: dagli impianti a terra ai sistemi satellitari' (2018) Rivista del diritto della navigazione 181; L. Trovò, 'Il processo d'integrazione degli spazi aerei europei: dalla riorganizzazione in blocchi funzionali verso la globalizzazione dell'Air Traffic Management (ATM)' (2011) IX Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente 439.

[15] Regulation (EU) No. 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No. 876/2002 and Regulation (EC) No. 683/2008 of the European Parliament and of the Council. Cf S. Andries, 'The European Initiative Galileo: A European Contribution to the Global Navigation Satellite System (GNSS)' (2000) XXV Annals of Air and Space Law 43; S. Hobe and J. Cloppenburg, 'Financial Contribution of Participating States to Optional Programmes of the European Space Agency (ESA). The Example of Galileo Sat Programme' (2003) Zeitschrift für Luft und Weltraumrecht 297; A. Masutti, 'Il Progetto Galileo (GNSS – Global Navigation Satellite System): garanzie di maggiore sicurezza negli aeroporti europei e relative implicazioni giuridiche', in *La sicurezza negli aeroporti. Problematiche giuridiche ed interdisciplinari* (Giuffrè 2005) 101 ff.; A. Roma, 'Recenti sviluppi del programma Galileo e delle sue applicazioni (Progetto EGNOS)' (2005) The Aviation & Maritime Journal 3; Magnosi (n 11), 82 ff.; Magnosi (n 14), 183 ff.; M. E. De Maestri, *La gestione pubblica del sistema Galileo e la responsabilità civile: questioni di giurisdizione, immunità e legge applicabile*' (2014) Il Diritto marittimo 288; Smith (n 10), 561 ff.

[16] See Articles 3 and 7-9 of the Regulation (EU) No. 1285/2013.

international conventions, governing liability, are currently in force, and they can be considered as a basic reference for the drafting of an appropriate legislation. So, we can refer to the two-tier liability regime, provided for in the Montreal Convention 1999 on international air transport,[17] or the strict liability regulation laid down in the Rome Convention 1952, on damages to third parties caused by an aircraft in flight.[18] Through the analysis of these and other matters it can be possible to elaborate and adopt a long-term legal framework, capable of guaranteeing certainty for operators and effective protection of users' rights.

5. *Satellite Navigation Systems and International Space Law*

The use of satellite technologies in the field of air traffic services also highlights the issue of the relevance of international law of outer space in this context. As we know, two specific Treaties provide a basic legal regulation governing liability arising from outer space activities: The Outer Space Treaty 1967[19] and the Washington Convention 1972, on damages caused by space objects (also called Liability Convention).[20] In particular, according to the provisions of the Liability Convention, damage caused by a space object (or its component parts) must consist of a physical

[17] Convention for the unification of certain rules for international carriage by air, signed at Montreal on 28 May 1999 and entered into force on 4 November 2003. The regime of liability is stated in the Chapter III: "Liability of the Carrier and Extent of Compensation for Damage". Art. 21 establishes a strict liability of the carrier for damages caused to a passenger on aircraft, with an upper limit of 113.100 SDR (Special Drawing Rights). In the other cases the article itself provides for a compensation on a fault-based liability. Cf. L. Tullio (ed.), *La nuova disciplina del trasporto aereo. Commento della Convenzione di Montreal del 28 maggio 1999* (Jovene 2006); Lefebvre d'Ovidio, Pescatore and Tullio (n 4), 512 ff.

[18] The Rome Convention on damage caused by foreign aircraft to third parties on the surfaces was signed on 7 Oct. 1952 and entered into force on 4 Feb. 1958. According to Art. 1 of the Convention, any person who suffers damage on the surface shall, upon proof only that the damage was caused by an aircraft in flight or by any person or thing falling therefrom, be entitled to compensation. See G. Romanelli, *I danni da aeromobili sulla superficie* (Giuffrè 1970); Ballarino and Busti (n 1), 314 ff.; E. Turco Bulgherini, 'Responsabilità per danni a terzi sulla superficie', in *Digesto delle discipline privatistiche Sezione commerciale* (Vol. 12, UTET 1996) 406 ff.; Lefebvre d'Ovidio, Pescatore and Tullio (n 4), 661 ff.

[19] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, done at Moscow, London, Washington on 27 Jan. 1967 and entered into force on 10 October 1967. See B. Cheng, 'The 1967 Space Treaty' (1968) Journal du Droit International 532; B. Cheng, *Studies in International Space Law* (Oxford University Press 1997), 97 ff.; N. Mateesco Matte, *Droit aérospatial, de l'exploration scientifique à l'utilisation commerciale* (Pedone 1976), 15 ff.; E. Back Impallomeni, *Spazio cosmico e corpi celesti nell'ordinamento internazionale* (CEDAM 1983), 21 ff.; Ballarino and Busti (n 1), 146 ff. M.G. Spada, *Diritto della navigazione aerea e spaziale* (Giuffrè 1999), 171 ff.; F. Von Der Dunk, 'International Space Law', in F. Von Der Dunk and F. Tronchetti (eds.), *Handbook of Space Law* (Elgar 2015) 29 ff.

[20] Convention on International Liability for Damage Caused by Space Objects, done at London, Moscow, Washington on 29 March 1972 and entered into force on 1 Sept. 1972, Cf. Mateesco Matte (n 19), 189 ff.; C. Christol, 'International Liability for Damage Caused by Space Objects' (1980) American Journal of International Law 346; M. Pedrazzi, *Danni causati da attività spaziali e responsabilità internazionale* (Giuffrè 1996); S. Magnosi, '2009 Space Odissey: spunti dal caso della collisione satellitare Russia – Stati Uniti del 10 febbraio 2009', in U. La Torre and A. L. M. Sia (eds) *La sicurezza nel trasporto e nelle infrastrutture della navigazione marittima ed aerea* (Rubbettino 2011) 335 ff.

and material collision.[21] This is today the prevailing interpretation of the regulation contained in the Convention. Otherwise, damage caused by satellite navigation systems may result from a malfunction or interruption of the signal emitted by satellite constellations. Even if the status of satellite signals has never been determined in law, it is nevertheless very difficult to consider the signal as a component part of the space object.

With regard to the Outer Space Treaty, Articles VI and VII prescribe that each Contracting State undertakes to authorize and supervise its respective national space activities. But satellite navigation, as said above, is a very complex system. Its numerous and various operations and applications take place in different contexts simultaneously: outer-space, airspace and ground-based instruments and procedures; aeronautical and surface activities. The satellite segment is just one of the components, that all form integral parts of the services offered by the global navigation satellite systems. For this reason, it seems appropriate to stress, once again, in conclusion, the need to elaborate and adopt specific international rules, capable of operating at different levels of relations and activities. This legal framework should take into account producers, operators and, last but not least, users.

[21] The Liability Convention distinguishes two categories of liability of the Launching State: strict liability for damages caused by a space object on the surface of the earth or to aircrafts in flight, fault liability in the other events of damage (Articles 2 and 3).

A NEW INTERNATIONAL LEGAL FRAMEWORK FOR UNMANNED MARITIME VEHICLES?

ANDREA CALIGIURI

SUMMARY: 1. Introduction. – 2. Types of UMVs. – 3. The legal status of UMVs. – 3.1. UMV as "ship/vessel". – 3.2. UMV as "device" or "equipment". – 4. UMVs with lethal autonomous capabilities: legal implications for such characterization.

1. *Introduction*

Unmanned maritime vehicles (UMVs) in operation today are essentially used for marine scientific research and military purposes; however, their number has risen exponentially in recent years and so has the number of research projects aimed at developing the first unmanned merchant ships.[1] At least 40 countries have invested in important projects for developing UMVs employed in coastal surveillance and patrolling, in search and rescue operations, in the maritime industry and in combat operations.[2]

Potential benefits of these UMVs are many:

a) operational safety: reduction of the amount and severity of accidents due to both a lack of crew on-board and the better performance that unmanned vehicles deliver;

b) reduction of costs: it is estimated that crew costs typically account for around 20-30% of the total cost for a cargo ship journey; but UMVs may increase onshore costs in the form of large upfront investments and upkeep of control and operations centers, sensors, data servers and communication assets such as high-bandwidth satellites;

c) energy efficiency and environmental impact: removal of human crews would allow UMVs to be lighter in size, reducing fuel consumption and pollution;

d) security: UMVs can be constructed so that it is difficult to board them, with cargo access and manual controls made unavailable and, in the event of a piracy, control centers could immobilize the ship or have it sail a specific route until naval authorities can reach it; without the presence of a crew to hold hostage for ransom, a cargo ship should be less valuable target.

In combat operations, the reasons for employing UMVs are primarily the achievement of a military advantage and the reduction of human losses.

However, employment of UMVs implies many challenges concerning their international regulation. The aim of this paper is to discuss the various UMV status

[1] Several autonomous cargo ship projects were in development, the most prominent one is the construction of the *MV Yara Birkeland*, a project by Norwegian companies Kongsberg and Yara International.

[2] The growing importance of this technology has also been affirmed by the Chinese government in the launch of the "Vision for Maritime Cooperation under the Belt and Road Initiative" calling States to intensify cooperation in the field of unmanned vessels (see <www.xinhuanet.com/english/2017-06/20/c_136380414.htm>).

alternatives and the legal consequences of each potential status determination. Before developing this analysis, it seems useful to offer a classification of UMVs.

2. *Types of UMVs*

There is a range of terminology used when discussing UMVs depending on the degree of autonomy these maritime vehicles have (remotely-operated UMV or autonomous UMV), whether they are below or above the sea (unmanned underwater vehicle (UUV) or unmanned surface vehicle (USV)), and whether they are intended for commercial or military use.[3]

International law does not define UMVs. However, in this paper, for having a factual understanding of the legal issues, we will borrow the definition of UMVs from the 2017 *U.S. Commander's Handbook on the Law of Naval Operations*. This document defines unmanned surface vehicles (USVs) as follow:

> "are watercraft that are either autonomous or remotely navigated and may be launched from surface, subsurface, or aviation platforms. The anticipated stealth, mobility, flexibility of employment, and network capabilities of USVs are expected to make them extremely valuable as force multipliers, particularly in the littoral environment. Potential missions envisioned for USVs include laying undersea sensor grids, antisubmarine warfare (ASW) prosecution, barrier operations, sustainment of carrier operating areas, mine countermeasures (MCM), intelligence, surveillance, and reconnaissance (ISR), bottom mapping and survey, and special operations support"

and it defines unmanned underwater vehicles (UUVs) as follow:

> "underwater craft that are either autonomous or remotely navigated and may be launched from surface, subsurface, or aviation platforms. Towed systems, hard-tethered devices, systems not capable of fully submerging such as USV, semi-submersible vehicles, or bottom crawlers are not considered UUVs. The sea services may employ UUVs for a wide variety of missions, including, but not limited to: ISR, MCM, ASW, Surveillance, Inspection/Identification, oceanography, communication/navigation network nodes, payload delivery, information operations (IO), time critical strike, barrier patrol (homeland defense, antiterrorism/force protection), and barrier patrol (sea-base support)".

Thus, in this paper, the term "unmanned" refers to both "remote controlled operation" as well as "autonomous operation".

[3] It is interesting to note that in China UMVs are mostly referred to as "intelligent ships", defined as "ships which automatically perceive and obtain information and data on ship itself, marine environment, logistics and port by making use of sensors, communication, the Internet of Things, the Internet and other technical means, and achieve intelligent operation in terms of ship navigation, management, maintenance and cargo transportation based on computer technology" (see China Classification Society, *Rules for Intelligent Ships* (2015), para. 1.1.3, <www.ccs.org.cn/ccswzen/font/fontAction!downloadArticleFile.do?attachId=4028e3d65494918801569776b4f503e8>).

The analysis that follows is based upon an assumption that UMVs are separate entities from their deploying platform and, therefore, they have a separate and independent legal regime from the latter.

3. *The legal status of UMVs*

On 15 December 2016, the Chinese PLA Navy seized an unmanned underwater vehicle (UUV) controlled by an American ship, the *USNS Bowditch*, an oceanographic survey ship, 50 nautical miles in the Philippine economic exclusive zone (EEZ) in the South China Sea. China had not made it clear on what legal basis it acted, although statements attributed to the Chinese government associated the legality of the capture of the drone with the absence of clearly written rules, as well as to the provocation by the USA through repeated "reconnaissance" in waters over which China claims its jurisdiction.[4] In response, the U.S. government called upon China to return the UUV immediately, stating that the *USNS Bowditch* and the UUV "were conducting routine operations in accordance with international law" and that the UUV was "a sovereign immune vessel of the United States".[5] The incident was finally resolved quickly and peacefully with the return of the drone about a week later.[6]

The *Bowditch* incident shows the uncertainty that exists in international law regarding the legal qualification of UMVs.

It is necessary to distinguish three main international regulatory areas from which the legal nature of UMVs can be inferred. First, there are rules on jurisdiction that establish the rights and obligations of States to take measures on ships; these rules are mainly set out in the UN Convention on the Law of the Sea (UNCLOS, 1982). Secondly, there are technical regulations concerning safety, environment training and watchkeeping standards etc., generally prescribed in conventions adopted by specialized UN agencies, such as, notably, the International Maritime Organization (IMO). Thirdly, there are a number of international standards in the field of private maritime law that have been established to harmonize issues such as the civil liability of shipowners for pollution, collisions or cargo-related losses and how such claims may be enforced.

The objective of this paper is to demonstrate that UMVs could be qualified as "ships" or "vessels" to which the existing customary and conventional international rules apply.

3.1. *UMV as "ship/vessel"*

In general, the variation between manned vehicles and unmanned vehicles, such as size of the means of propulsion, type of platform, capability, endurance, human versus

[4] J. Borger, 'Chinese warship seizes US underwater drone in international waters' (16 December 2016) The Guardian <https://www.theguardian.com/world/2016/dec/16/china-seizes-us-underwater-drone-south-china-sea>.

[5] Statement by Pentagon Press Secretary Peter Cook on Incident in South China Sea, 16 December 2016 <https://www.defense.gov/Newsroom/Releases/Release/Article/1032611/statement-by-pentagon-press-secretary-peter-cook-on-incident-in-south-china-sea>.

[6] Statement by Pentagon Press Secretary Peter Cook on Return of U.S. Navy UUV, 19 December 2016 <https://www.defense.gov/Newsroom/Releases/Release/Article/1034224/statement-by-pentagon-press-secretary-peter-cook-on-return-of-us-navy-uuv>.

autonomous control and mission set, has not been regarded as a defining element of what constitutes a "vessel" or "ship."

The 1982 UNCLOS uses the terms "ship" and "vessel" interchangeably, without providing a definition. Its Art. 91, which explicitly describes certain legal characteristics of a "ship", underlines a "genuine link" that must exist between a State and its ship; this link is manifested through the granting by the State of its nationality to the ship, the registration in its territory and the right to fly its flag.

If these were the characteristics to define a ship, an UMV could be qualified as a ship because it generally has a nationality, is registered in the shipping registers of a State and flies a national flag.

A part of the doctrine has always believed that the absence of a definition of "ship" in UNCLOS was linked to the fact that it referred to the notion enclosed in maritime conventions which have an almost universal adhesion. However, it should be noted that the latter conventions provide varying definitions of "ship" or "vessel" that are functionally limited.

Some of these maritime conventions stress that a ship is used or capable of being used as a means of transportation on water;[7] others provide a broad definition referring to any type of vessel;[8] finally, the SALVAGE Convention states that "vessel" means any ship or craft, but also "any structure capable of navigation".[9]

Since there is no universally accepted understanding of "means of transportation on water", an UMV could fall within the notion of ship. Indeed, if it is assumed that transportation has a functional value, the functional definition could include transportation of payloads, weapons systems, or internal sensors and so UMVs, by design, meet this definition.[10]

There are some maritime conventions that accept a broad notion of ship, such as the SOLAS Convention, hence it is possible to assert that in principle UMVs may technically be regulated by SOLAS but, in practice, they are unable to comply with many of the Convention's rules, in particular with those provisions given by human-centered obligations.[11]

[7] See Rule 3 Convention on the International Regulations for Preventing Collisions at Sea (COLREGs, 1972); Art. 2 UN Convention on Registration of Ships (1986); Art. 1(d) Hague Rules (as amended by the Brussels Protocol 1968).

[8] See e.g. in Art. 2(4) of the International Convention for the Prevention of Pollution from Ships (MARPOL, 1973), "ship" means a vessel of any type whatsoever operating in the marine environment and includes hydrofoil boats, air-cushion vehicles, submersibles, floating craft and fixed or floating platforms". Obviously, this full definition includes unmanned ships. See also Art 1(6) Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Matte (London Convention, 1972); Art. 2(3) International Convention on oil pollution preparedness, response and cooperation (1990); Art. 1 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA, 1988). It is to note that the International Convention for the Safety of Life at Sea (SOLAS, 1974) does not give a single definition of ship or vessel, but "all ships" means any ship, vessel and crafts irrespective of type or purpose.

[9] Art. 1(b) International Convention on Salvage (1989).

[10] C. H. Allen, 'Determining the Legal Status of Unmanned Maritime Vehicles: Formalism vs Functionalism' (2018) 49 Journal of Maritime Law and Commerce 477, 496.

[11] L. Giunta, 'The enigmatic juridical regime of unmanned maritime systems', in *OCEANS 2015 – Genova*, (IEEE 2015) 1; Li Rui, 'On the legal status of unmanned ships' (2019) China Oceans Law Review 165.

From the above mentioned examples we could gather that it does not seem to be essential to defining a "ship" that it has a master or crew onboard, so UMVs would mostly be covered by existing regulatory definitions, and the existing conventions would continue to be functional for what concerns them.

However, the potentially confusing notion of "ship" or "vessel" does not contribute to defining the legal regime applicable to UMVs.

The problem is not negligible if the IMO is currently studying existing conventional instruments to assess how they could be applied to UMVs (see the so-called "Maritime Autonomous Surface Ships (MASS) project").[12] Options under study are to amend the existing maritime conventions to include an explicit reference to MASS; to negotiate a new Convention covering all aspects of the existing maritime conventions but applicable to MASS; to define a MASS Code of Conduct referring to the relevant maritime conventions; or to apply the existing conventions to MASS by "equivalent". The last option seems to be the most practicable, because amending existing conventions or negotiating a new convention would require a very long time frame for the creation of rules also applicable to UMVs. Nevertheless, the adoption of a Code of Conduct by the IMO could have little effect given the non-binding nature of such an instrument.

A more general argument can be made by recognizing an "evolutionary approach" to treaty interpretation. Under Art. 31(1) of the Vienna Convention on the Law of Treaties, a treaty must be interpreted in good faith and "in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose". In this regard, the International Court of Justice has found that where a generic term is used – in that particular case, the term "commerce" – and where the relevant provision aims to settle a matter for an indefinite duration, treaty terms "must be understood to have the meaning they bear on each occasion on which the Treaty is to be applied, and not necessarily their original meaning"[13]. Thus, if, in the context of a treaty signed in the XIX century, the term "commerce" can be interpreted in an evolutive way to include "tourism", it is reasonable to assume that the term "ship" under UNCLOS can include new types of ships as well as UMVs.[14]

[12] IMO initiated a regulatory scoping exercise for the use of MASS. These scoping exercises are conducted by the Maritime Safety Committee (see IMO, 'Report of the Maritime Safety Committee on its 98th Session' (28 June 2017) IMO Doc MSC 98/23, para 20) and the Legal Committee (see IMO 'Report of the Legal Committee on the Work of its 105th Session' (1 May 2018) IMO Doc LEG 105/14, para 11.7-11.11); each Committee considers the conventions falling within its purview. On the development of the MASS project, see Z. Pietrzykowski and J. Hajduk, 'Operations of Maritime Autonomous Surface Ship' (2019) 13 The International Journal on Marine Navigation and Safety of Sea Transportation 725.

[13] See International Court of Justice, *Costa Rica v Nicaragua (Dispute Regarding Navigational and Related Rights)* (2009)] I.C.J. Reports 213, paras. 70-71.

[14] Concerning the use of an "evolutionary approach" to interpret the UNCLOS, see International Tribunal of the Law of the Sea, *Request for an advisory opinion submitted by the Sub-Regional Fisheries Commission (SRFC)*, Advisory Opinion of 2 April 2015, Separate Opinion of Judge Lucky, para. 18: "[…] The 1982 Convention and the Statute of the Tribunal are "living instruments". This means that they "grow" and adapt to changing circumstances. An act/statute is always "speaking". The law of the sea is not static. It is dynamic and, therefore, through interpretation and construction of the relevant articles a court or tribunal can adhere and give positive effect to this dynamism. Since 1982, technology has advanced and therefore in my view judges must take a robust approach and apply the law in a legal but pragmatic way. […]".

This evolutive approach also responds to State practice expressed in national legislation and regulations[15] and in international fora. For instance, the IMO MASS project demonstrates that a broad majority of IMO member-States believe that at least some UMVs, the USVs, are "ships" and this view is confirmed by the majority of national maritime law associations which participated in the "Questionnaire on Unmanned Ships" proposed by the *Comité Maritime International* in 2017, which focused their responses on whether unmanned ships would be subject to UNCLOS and thus subject to the same rights and duties of manned ships.[16]

If UMVs can be considered ships or vessels, they must comply with UNCLOS navigation rules.

The entitlement to navigational rights appears strategically advantageous for those States with the capability to build and deploy UMVs on a large scale. For example, Articles 17 and 52 UNCLOS recognize the right of innocent passage, defined as a continuous and expeditious traversing of the territorial sea or archipelagic waters in a manner not prejudicial to the peace, good order, or security of the coastal or archipelagic State.[17] Here, when UMVs are exercising this right in compliance with the applicable law of the sea requirements, the coastal State may not prevent or interfere with their passage through its territorial or archipelagic waters.

UMVs also enjoy all other navigational rights in accordance with the international law of the sea: the transit passage in straits used for international navigation,[18] the archipelagic sea lanes passage[19] and the freedom of navigation in the EEZs[20] and in the high seas.[21]

However, the drone revolution has arrived at a period of intense maritime tension between several States; a period during which the navigation rules of the law of the sea are subject to interpretations that are not always well-accepted by all States. For instance, restrictions imposed by coastal States to navigation rights of foreign ships must be noted: a number of States require prior notification before a foreign warship may conduct innocent passage through their territorial waters; other States prohibit the passage of ships carrying nuclear and other weapons of mass destruction through their territorial seas, at least eighteen States purport to regulate or prohibit foreign military activities in their EEZs and a growing number of coastal States passed legislations and enacted unilateral measures to increase their control over the portion of waters of

[15] See, e.g., legislation of Belgium (Act of 21 December 1990 on the registration of ships, s.1(1)), England and Wells (Merchant Shipping Act 1995, s.313), France (Code des Transports, Art L.5000-2), Greece (Code of Public Maritime Law, Art. 3), The Netherlands (Burgerlijk Wetboek (BW), Book 8, Art 194), Poland (Maritime Code of 2001, Art 2(1)), Spain (Commercial Registration Regulation 1597/1989), Swede (Maritime Code, s. 2) and USA (US Code-Rules of Construction Act, Title 1, para. 3). See also Chinese regulations (China Classification Society, *Rules for Intelligent Ships* (2015) and *Guidelines for Autonomous Cargo Ships* (2018)).

[16] On the text of the Questionnaire and the Responses to the Questionnaire, see <https://comitemaritime.org/work/mass>. In particular, see responses by Dutch, Finnish, French, German, Panamanian and US maritime law associations.

[17] See Articles 18 and 19 UNCLOS.

[18] Art. 38 UNCLOS.

[19] Art. 53 UNCLOS.

[20] Art. 58(1) UNCLOS.

[21] Art. 87 UNCLOS.

international straits within the limit of their maritime zones. All these restrictions are supposed to be extended to UMVs.

3.2. *UMV as "device" or "equipment"*

If an UMV, by design, cannot be considered a "ship" or a "vessel" under the law of the sea, it could be considered something else, such as a "device" or "equipment".

UNCLOS Part XII, entitled "Protection and preservation of the marine environment", refers to "device" in two provisions.

Art. 194(3), concerning measures to prevent, reduce and control pollution of the marine environment, designs these measures to minimize to the fullest possible extent, in its letter c), "pollution from installations and devices used in exploration or exploitation of the natural resources of the seabed and subsoil" and, in its letter d), "pollution from other installations and devices operating in the marine environment".

Art. 209(2), concerning pollution from activities in the Area, affirms that "States shall adopt laws and regulations to prevent, reduce and control pollution of the marine environment from activities in the Area undertaken by vessels, installations, structures and other devices flying their flag or of their registry or operating under their authority, as the case may be".

The wording of the two provisions suggests that some UMVs could fall under these provisions.[22]

In Part XIII, entitled "Marine Scientific Research", UNCLOS refers to "equipment". In particular, Art. 261 states that the deployment and use of any type of scientific research installations or equipment "shall not constitute an obstacle to established international shipping routes" and Art. 262 affirms that "Installations or equipment […] shall bear identification markings indicating the State of registry or the international organization to which they belong and shall have adequate internationally agreed warning signals to ensure safety at sea and the safety of air navigation, taking into account rules and standards established by competent international organizations".

Some UMVs used for marine scientific research purposes could undoubtedly be included among the "equipment" referred to in Part XIII.[23] However, their use is subject to certain restrictions, such as the obligation to provide information to the coastal state when operating in its EEZ or on its continental shelf according to Art. 248(b) and (d).

Some UNCLOS provisions define with a little room of ambiguity the legal regime of "device" and "equipment" in relation to navigation rights, establishing significant limits in the exercise of these rights.

For the right of innocent passage, two UNCLOS provisions are illustrative:

[22] Some UUVs could inspect oil and gas platforms in very deep waters; see e.g. the use of Saipem's Underwater Intervention Drone (UID) Hydrone-R and the all-electric Work Class ROV Hydrone-W in the Njord Field development <https://www.saipem.com/en/projects/hydrone-njord-field-development>.

[23] Examples of small UMVs employed for this purpose are "Saildrone" (it is a USV produced by the company Saildrone) and "Wave Glider" (unmanned robots produced by Liquid Robotics, a wholly owned subsidiary of The Boeing Company) for data collection in the fields of meteorology, oceanography, fisheries, tsunami and seismic monitoring and offshore operations monitoring.

a) Art. 17 concerning the discipline of this right makes clear that it is only available for maritime vehicles which can be qualified as "ships";[24]

b) Art. 20, which seems to entitle to some specific UMVs – UUVs – to exercise the right of innocent passage, provides that submarines "and other underwater vehicles" must operate on the surface and show their flag while in a foreign territorial sea. Thus, UUVs could be qualified as "other underwater vehicles" according to the UNCLOS; but Art. 20 is to be interpreted enclosed with Art. 17.

As with innocent passage, there is no support in UNCLOS for the proposition that a non-vessel "device" or "equipment" is entitled to exercise the right of transit passage in straits used for international navigation[25] and the archipelagic sea lanes passage,[26] both being regimes established for "ships".

However, when UMVs – as devices or equipment – operate on or under the high seas and in EEZs, there is little doubt that their use cannot be restricted.

4. *UMVs with lethal autonomous capabilities: legal implications for such characterization*

What happens if UMVs with lethal autonomous capabilities are operated by or under the exclusive control of the armed forces? Could they be qualified as "warships" under the law of the sea? What happens if they are merely military "devices" or "equipment"?[27]

Without the right to exercise navigational regimes available to "warships" granted by the law of the sea, the utility of UMVs to national navies would be significantly limited.

UNCLOS, in Art. 29, defines "warship" as:

> "[a] ship belonging to the armed forces of a State bearing the external marks distinguishing such ships of its nationality, under the command of an officer duly commissioned by the government of the State and whose name appears in the appropriate service list or its equivalent, and manned by a crew which is under regular armed forces discipline."[28]

[24] M. Nordquist (ed.), *United Convention on the Law of the Sea 1982 - A Commentary* (Vol. II, Martinus Nijhoff 2002), 180 ff.

[25] See above (n 18).

[26] See above (n 19).

[27] For commentary on the debate surrounding this issue, see M. N. Schmitt and D. S. Goddard, 'International law and the military use of unmanned maritime systems' (2016) 98 International Review of the Red Cross 567; R. Veal, M. Tsimplis, H. Nasu and D. Letts, 'The Legal Characterization of Lethal Autonomous Maritime Systems: Warship, Torpedo, or Naval Mine?' (2020) 96 International Law Studies 79; Y. Saito, 'Reviewing Law of Armed Conflict at Sea and Warfare in New Domains and New Measures: Submarine Cables, Merchant Missile Ships, and Unmanned Marine Systems' (2019) 44 Tulane Maritime Law Journal 107; R. McLaughlin, 'Unmanned Naval Vehicles at Sea: USVs, UUVs, and the Adequacy of the Law', (2011/2012) 21 Journal of Law, Information and Science 100; D. Amoroso, 'Jus in bello and jus ad bellum arguments against autonomy in weapons systems: A reappraisal' (2017) 43 QIL – Questions of International Law 5 <http://www.qil-qdi.org/jus-bello-jus-ad-bellum-arguments-autonomy-weapons-systems-re-appraisal>.

[28] This definition is derived from the 1958 Geneva Convention on the High Seas (Art. 8(2)), which in turn relied upon the definition used in the 1907 Hague Convention VII relating to the Conversion of Merchant Ships into Warships (Articles 1-4). The term warship includes submarines and surface ships,

At first glance, according to a literal interpretation, the UNCLOS provision suggests that UMVs are precluded from having the legal status of warships because there is no duly commissioned officer authorized to take command or a crew physically present on board.

In light of the limits imposed by UNCLOS to qualify a "warship", some scholars[29] have however suggested to look for the meaning of warship in customary international law and, in particular, accepting a broad notion of warship that would derive from an application by analogy of the concept of "military aircraft".[30]

On the contrary it might be argued that an UMV must be qualified as "other government ship operated for non-commercial purposes" and as such it would enjoy the same legal status of a warship under UNCLOS. In particular, according to Art. 31 UNCLOS, the flag State shall bear international responsibility for any loss or damage to the coastal State resulting from the non-compliance by an UMV, which is a government ship operated for non-commercial purposes, with the laws and regulations of the coastal State concerning passage through the territorial sea or with the provisions of UNCLOS or other rules of international law, and according to Art. 32 UNCLOS, an UMV, which is a government ship operated for non-commercial purposes, shall enjoy sovereign immunity.[31]

This interpretation complies with UNCLOS because the latter Convention does not give a notion of "other government ship operated for non-commercial purposes".

This interpretation is, for example, endorsed by the USA in the *Commander's Handbook on the Law of Naval Operations*. In this document, USVs and UUVs that are engaged exclusively in governmental, non-commercial service are covered by sovereign immunity and it is specified that their status is not dependent on the status of their launch platform.[32]

The issue of sovereign immunity becomes more difficult to resolve if UMVs do not qualify as ships; thus, for example, the *German Commander's Handbook* takes the position that UMVs enjoy sovereign immunity status to the extent that they are controlled from a ship which itself enjoys such status.[33]

as well as Coast Guard vessels that belong to the armed forces of the State (see 1995 San Remo Manual on International Law applicable to Armed Conflict at Sea).

[29] A. Norris, *Legal Issues Relating to Unmanned Maritime Systems* (U.S. Naval War College 2013) <https://www.hsdl.org/?view&did=731705>, 27 ff.

[30] See Rule 1(x) of the *HPCR Manual on International Law Applicable to Air and Missile Warfare (2009)*; this provision affirms: "'Military aircraft' means any aircraft (i) operated by the armed forces of a State; (ii) bearing the military markings of that State; (iii) commanded by a member of the armed forces; and (iv) controlled, manned or preprogrammed by a crew subject to regular armed forces discipline". This provision extends to all unmanned aerial vehicles, whether unarmed (UAV) or armed (UCAV), and whether remotely piloted or operating autonomously (see *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare (2010)*, par. 6, p. 47).

[31] See also Art. 96 UNCLOS.

[32] *Commander's Handbook on the Law of Naval Operations* (2017), para. 2.3.6 (Unmanned Surface Vehicle/Unmanned Underwater Vehicle Status).

[33] *German Navy, Commander's Handbook: Legal Bases for the Operations of Naval Forces*, SM 3, 2002, 45.

If a military UMV can be qualified as a "government ship operated for non-commercial purposes", like a "warship", it is entitled to all the navigational rights granted by UNCLOS.

Another consequence of the UMV status as "government ship" could be in the entitlement to perform certain important maritime functions when it is clearly marked and identifiable as being on government service and authorized to that effect,[34] including carrying out a seizure on account of piracy,[35] conducting a right of visit boarding[36] and engaging in hot pursuit of a foreign ship or its boats.[37] However, UMVs are able to perform only some components of these maritime functions. It is important to distinguish the vessel-like components of these maritime functions from the crew-like components. Thus, while a State may use UMVs to conduct some of the vessel-like functions (i.e. carrying a boarding team, conducting surveillance, pursuing a fleeing vessel, signaling such a vessel to stop), it cannot use these UMVs to carry out the crew-like components of these functions (i.e. physically boarding a vessel, conducting inquiries, conducting searches, seizures, and arrests).

In contrast, UMVs, qualified as military devices or equipment, are not entitled to exercise navigation rights in accordance with the UNCLOS,[38] except for the freedom of navigation in high seas and EEZs. Additionally, there is no question as to the impossibility for UMVs, qualified as military devices or equipment, to be entitled to perform those important maritime functions expressly reserved for warships and other duly authorized ships.

Nevertheless, the legal status of "warships" is clearly distinct from "other governmental ships" during an international armed conflict in that only warships are entitled to exercise belligerent rights.[39]

Assuming the validity of this principle, it further follows that only warships could be directly targetable by opposing belligerent forces; otherwise, as a non-warship, an UMV may be stopped, visited, and searched,[40] and also seized[41] if of enemy nationality, but not attacked as a measure of first resort. This limitation on attack of a non-warship does not preclude such a vessel/craft from defending itself if attacked.[42] However, any participation in hostilities in any manner whatsoever by a non-warship subjects it to attack by a belligerent warship.[43] In addition, if the interpretation of the term

[34] For an in-depth analysis on this topic, see N. Klein, 'Maritime Autonomous Vehicles within the International Law Framework to Enhance Maritime Security' (2019) 95 *International Law Studies Series* 244.

[35] Art. 107 UNCLOS.

[36] Art. 110 UNCLOS.

[37] Art. 111 UNCLOS.

[38] See Art. 19(f) UNCLOS, which clearly affirms that passage of a foreign ship in territorial waters of a third State shall be considered to be prejudicial to the peace, good order or security of the coastal State if in the territorial sea it engages in "the launching, landing or taking on board of any military device". Thus, an UMV as military device has no right to an innocent passage.

[39] See *Manual of the Laws of Naval War, adopted by the International Institute of International Law*, 9 August 1913. Although this manual is not a treaty, its provisions are largely reflective of customary international law.

[40] Art. 32, Manual of the Laws of Naval War (1913).

[41] Art. 33, Manual of the Laws of Naval War (1913).

[42] Art. 12, Manual of the Laws of Naval War (1913).

[43] Art. 49, Manual of the Laws of Naval War (1913).

"hostilities" in the aviation realm carries over to the maritime realm, even the collection of information by an UMV could subject it to attack by an enemy warship.

Although it is difficult to characterize UMVs as warships, an UMV could be a "means of warfare" (weapons and weapons systems) as a "device" or "equipment" to the extent that it is capable of engaging in an activity which qualifies as an "attack", such as anti-surface, anti-submarine or mine-laying operations.

Art. 36 of the Additional Protocol I to the Geneva Conventions and relating to the Protection of Victims of International Armed Conflicts (AP I) provides that:

> "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party".

According to this provision, the High Contracting Parties undertake determining the possible prohibition of a new weapon, both with regard to the provisions of the Protocol and any other applicable rules of international law, on the basis of the normal use foreseen at the time of the evaluation.

The purpose of Art. 36 is to ask States whether the normal or intended use of a new weapon would be unlawful in some situations or in all circumstances. A State is not required to foresee or study all possible misuses of the weapon in question, since almost all weapons could have misuses that are prohibited.[44]

The employment of UMVs as "means of warfare" entails the compliance with principles and rules of law of armed conflicts concerning the conduct of hostilities,[45] in particular, distinction, proportionality, and the obligation to take all feasible precautions.[46]

A party to the conflict employing an UMV to conduct an attack must assess whether that attack is directed at a lawful target. A special regime for "military objectives" exists at sea.[47] Certain ships are immune from direct attack, protected from indiscriminate attack, included in proportionality calculations, and considered vis-à-vis the requirement to take precautions in attack during maritime operations.[48]

[44] It must be noted that there are some problems for applying international humanitarian law, in particular concerning its prohibitions, when UMVs are qualified as "devices", for example as "torpedoes" or "naval mines". On this issue, see Veal, Tsimplis, Nasu and Letts (n 27).

[45] See *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, 12 June 1994. Although this manual is not a treaty its provisions are largely reflective of customary international law.

[46] See respectively Rules 39, 41 and 46.

[47] See Rule 47, San Remo Manual.

[48] Art. 57(4), Additional Protocol I: "In the conduct of military operations at sea or in the air, each Party to the conflict shall, in conformity with its rights and duties under the rules of international law applicable in armed conflict, take all reasonable precautions to avoid losses of civilian lives and damage to civilian objects".

CONNECTED AND AUTOMATED MOBILITY OF ROAD VEHICLES

CARMEN TELESCA

SUMMARY: 1. Introduction. – 2. The State of the art on the development of self-driving vehicles in Europe and Italy. – 3. Prospects for reform in the field of motor vehicle liability. – 4. Concluding remarks.

1. *Introduction*

The road haulage sector and, more generally, the mobility sector are an integral part of a rapidly evolving system capable of outlining new perspectives to be implemented and regulated by the legislator.

The introduction of self-driven vehicles, as a solution applicable to both public and private mobility, raises a number of legal and ethical questions in the face of an ever-increasing development of the technological sector.

The peculiar use of artificial intelligence in the road traffic sector has already been the subject of interest in recent years by the Member States of the European Union: in 2016, in fact, the "Declaration on cooperation in the field of connected and automated driving" was signed with the aim of facilitating the process of creating and marketing completely autonomous vehicles through the identification of a common regulatory framework to achieve perfect cohesion between vehicles and infrastructure, in full compliance with road safety rules.

From a defining point of view, self-guided vehicles can generally be qualified as those vehicles in which the driver can delegate certain functions (e.g. accelerating, steering, etc.) to the computerised system through a series of technological supports (e.g. Global Positioning System, sensors, etc.) that allow the vehicle to interface both with other users and with the road infrastructure.

In the most advanced form, with the increased potential of automation and connectivity, the driver, through a completely autonomous system, can be excluded from driving.[1]

The different levels of autonomous driving are qualified as the stages of technological evolution linked to this sector.[2]

[1] Cf. the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, On the road to automated mobility: An EU strategy for mobility of the future, COM (2018) 283 final, 17 May 2018, where it is underlined that "The ability of vehicles to communicate will be key to integrate automated vehicles in the overall transport system. The different types of communication technologies are complementary and evolving over time with improvements (for example in coverage, speed, latency, security). This enables more and more advanced use cases of automated vehicles. Although most of the investment for connectivity should come from the private sector, the EU can help in providing regulatory approaches that foster the investments needed in vehicles and communication infrastructure (road and telecoms). [...]". Cf. L. Butti, 'Auto a guida autonoma: sviluppo tecnologico, aspetti legali ed etici, impatto ambientale' (2016) Rivista giuridica dell'ambiente 435.

[2] The proposal for a classification of vehicles on the market, in relation to a more or less high level of automation, was drawn up by the European Parliament, within the Directorate-General for Internal

In view of this, a distinction must be made between partially automated and fully autonomous driving operations in order to correctly classify problems concerning safety and responsibility profiles. For semi-automatic vehicles (automation levels one to four), the driver is assisted by new technologies (e.g. radar, laser, etc.), while in cars with autonomous driving (level five), as already highlighted, it is not at all essential that there is a driver. It follows from this situation that, in the case of semi-automatic vehicles, the driver remains responsible in all circumstances, while in the case of totally autonomous driving the question of responsibility is more complex and it requires appropriate in-depth studies and ad hoc regulatory interventions by the legislator.

2. *The state of the art on the development of self-driving vehicles in Europe and Italy*

In terms of connected and automated mobility, the scenario, at European level, is quite varied. The European Commission, on 17 May 2018, presented the third mobility package, completing the process that had started in 2016 with the guidelines for mobility towards the low emission target and the two previous "Europe on the move" packages of 2017.[3]

The package mainly concerns road transport, which is analysed in relation to some specific aspects that can be traced back to automation, safety, and emission control for a more widespread protection of the environment.

The European Commission, in support of automation in the transport system, has developed a series of measures to encourage connectivity and infrastructure services.[4]

Specifically, the path identified by the Commission foresees the achievement of fully automated mobility for cars, trucks, and public transport sector by 2030.

Policies, Policy Department B: Structural and Cohesion Policies, Transport and Tourism, as part of the study 'Research for TRAN Committee – Self-piloted cars: the future of road transport?', 2016 <www.europarl.europa.eu>. In the United States, on the other hand, this classification has been adopted by the Department of Transportation and, moreover, it has been drawn up by the US standardisation body for the automotive and aerospace sectors, the so-called SAE International.

[3] With the third mobility package (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, Europe on the move. Sustainable Mobility for Europe: safe, secure, connected and clean,* COM (2018) 293 final, 17 May 2018?, the Commission's main objective is to "ensure a smooth transition towards a mobility system which is safe, clean and connected & automated. [...] The Commission is committed to supporting Member States in systematically identifying dangerous road sections and better targeting investment. According to the Commission, these two measures could save up to 10,500 lives and avoid 60,000 serious injuries over the period 2020-2030, contributing to the EU's long-term target of zero fatalities and serious injuries by 2050 (Vision Zero and Safe System approach)".

[4] The following communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions are exemplary in this respect: 5G for Europe: An Action Plan, COM (2016) 588 final, 14 September 2016; the communication Space Strategy for Europe, COM (2016) 705 final, 26 October 2016; and the communication A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, COM (2016) 766 final, 30 November 2016. With reference to the development of Cooperative Intelligent Transport Systems (C-ITS), the European Commission has adopted new rules.

The first step, to be completed by 2022, will be to ensure a perfect connection (via the internet) between self-driven vehicles that have to be able to interact with each other and with the external environment.[5]

With the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, On the road to automated mobility: An EU strategy for mobility of the future,[6] it is hoped that the European Union will be able to achieve a uniform approach for the implementation of a mobility towards automation and, to this end, it will direct Member States towards the necessary actions for the adaptation of "basic services and infrastructures", also because the infrastructures dedicated to the operation of autonomous vehicles differ widely in each of the EU countries.

In this perspective, the Commission will also have the task of assessing, over time, the benefits of automation, both from a socio-economic and environmental point of view, in the whole transport sector through a regular joint analysis with the interested parties.

Following on from the work started by the Commission, the European Parliament, on 15 January 2019, adopted a non-binding resolution on self-driving in the whole maritime and inland waterway, air, rail, road transport sector with the primary aim of protecting users' and consumers' rights as well as the principles of transparency and competition.[7]

Among the Member States of the European Union, Germany was one of the first countries to adopt specific legislation in 2017 through a new road traffic law (*Straßenverkehrsgesetz* – StVG) covering vehicles with a high degree of automation and those with fully autonomous driving.[8]

The aim of this law is to achieve an "intelligent" mobility by raising road safety levels and controlling vehicle emissions in order to protect the environmental impact. First of all, in pursuit of these aims, the German legislator has modified the definition of motor vehicle as it is extended to motor vehicles driven either highly or fully automated.[9]

The concept of driver has also been reviewed, including, pursuant to Art. 1 of the StVG, anyone who activates a highly or fully automated driving function, i.e. anyone who for a certain period of time entrusts the control of the vehicle to the

[5] The European Commission, also in the above-mentioned Communication of 17 May 2018, COM (2018) 283 final, with reference to freight transport, has also proposed the creation of an exclusively digital platform to be used to facilitate the exchange of information, which will also produce benefits in the logistics sector, with the main aim of reducing the existing high degree of bureaucracy.

[6] See above (n 1).

[7] European Parliament resolution of 15 January 2019 on independent driving in European transport (2018/2089 (INI)), P8_TA(2019)0005.

[8] It is the Road Traffic Act (StVG) of 16 June 2017, which came into force on 21 June 2017. See Mario G. Losano, 'Il progetto di legge tedesco sull'auto a guida automatizzata' (2017) XXXIII Diritto dell'Informazione e dell' informatica 1.

[9] The reference contained in the Art. 1 of the StVG refers to vehicles equipped with special technical devices that make it possible to control driving after their activation and to comply with general traffic regulations. These systems can be deactivated directly by the driver and can also provide clear instructions to the driver by means of acoustic and optical signals, etc.

computerised system, while remaining physically in the passenger compartment of the vehicle.[10]

It should be noted that in the United Kingdom, in fact, a specific regulation on *Self-Driving Vehicles* (SDVs) was drawn up in 2015 and updated in February 2019 through the adoption of the *Code of Practice: Automated vehicle trialling*, which specifies the methods and conditions for testing SDVs.[11]

The *Code of Practice: Automated vehicle trialling* identifies the requirements for testing and specifies that "trialling any level of automated vehicle technology is possible on any UK road if carried out in line with UK law. Trialling organisations do not need to obtain permits or pay surety bonds when conducting trials in the UK. As part of complying with the law, they will need to ensure that they have: a driver or operator, in or out of the vehicle, who is ready, able, and willing to resume control of the vehicle; a roadworthy vehicle; and appropriate insurance in place". A further safeguard element in the testing phase is the necessary presence of an operator who can control the vehicle remotely where there is no driver inside the vehicle.

Significant examples of testing in the driverless cars sector are also recorded in countries outside the European Union. In the United States, in fact, there are car companies that, for several years now, have been testing automated vehicles even though their use on the road is not yet permitted in some states, so much so that a bill to adopt the Self-Drive Act is currently being discussed in Congress to uniformly regulate the homologation of this type of vehicle in all federal states.

Even in Canada, in the Ontario region, testing for SDVs was initiated and regulated by the Ontario Regulation 306/15 Pilot Project-Automated Vehicles and subsequently amended in January 2019. The Canadian test example always requires a driver, with special authorisation, to be on board the vehicle and to create easily accessible systems for deactivating the autopilot or signalling possible problems so that the driver can easily regain control of the driving functions.[12]

Similar experiences can also be seen in Singapore, where, as early as 2017, the Ministry of Transport amended the Road Traffic Act by including specific provisions for self-driven vehicles that require, in this country too, the presence of a driver on board, as a precautionary measure, if there are contingent problems that need to be solved.

Also in Italy, in recent years, a lot of progress has been made and with the decree of the Ministry of Infrastructure and Transport (hereinafter "Mit") No. 70 of 28 February 2018 (the so-called "Smart Road"), road testing for connected and automatically driven vehicles has been authorised.[13] The prospect is, first and foremost, that of upgrading the motorway network, with the expectation of charges to

[10] In any case, the driver is still obliged to take control of the vehicle immediately in special cases (e.g. malfunction of the acoustic and tactile devices, prohibitive weather conditions, etc.).

[11] The text of the Code of Practice: Automated vehicle trialling issued by the Department for Transport and the Centre for Connected and Autonomous Vehicles is available at <https://www.gov.uk/dft>.

[12] For more information on the US experience see the website <http://www.congress.gov/115th-congress/house-bill/3388>. The text of the Ontario Regulation 306/15 Pilot Project-Automated Vehicles is available at <http://www.ontario.ca/laws/regulation/150306>.

[13] Decree No. 70 of the Ministry of Infrastructure and Transport of 28 February 2018, called *Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di Smart Road e di guida connessa e automatica* (the so-called *Smart Road*), in *Gazzetta Ufficiale* No. 90, 18 April 2018.

be borne by the concessionaire or the operator. On 4 October 2018, the Italian technical support observatory for *Smart Road* and connected and automatically driven vehicles also approved the forms for the request to the Mit for the authorisation to test these vehicles on public roads and to obtain the prior authorisation of the managing body of the infrastructure section on which the test is to be carried out.[14]

The testing of automatically driven vehicles on public roads is authorised by the General Directorate for Motorisation of the Ministry of Infrastructure and Transport after receiving a positive opinion from the Technical Support Observatory for *Smart Road*. The first authorisation for the experimentation on public roads of the first self-driven vehicle in Italy was officially issued on 7 May 2019, and it states that the competent management of the Mit has successfully completed the necessary preliminary checks of suitable technical age for the circulation of the tested vehicle, of VisLab S.r.l., created as a spin-off of the University of Parma and acquired, in 2015, by the US company Ambarella Inc. The experiment, after about a year from its beginning, had a positive outcome and concerned the urban area and the last mile type D, E, F of precise road sections in the cities of Turin and Parma, in compliance with all the requirements laid down by the road operator and in the presence of a supervisor able to switch between automatic and manual operation of the vehicle, so as to guarantee, in all circumstances, maximum respect for safety.

3. *Prospects for reform in the field of motor vehicle liability*

The starting point, in order to analyse the profiles of responsibility, arises from a question: to verify whether the Italian legislation can be considered already prepared in the management of the regulation of the circulation of driverless and highly automated driving vehicles, or whether, instead, it is necessary an intervention by the legislator that affects, with amendments and/or additions, the legal regulations in force.

The resolution of the issue concerns, in particular, fully autonomous driving vehicles (level five) and highly automated driving vehicles, which can be driven

[14] The para. 2 of Art. 9 of the aforementioned Ministerial Decree No. 70/2018 provides that authorisation to test automatic driving vehicles on public roads *may be requested, individually or jointly, by the manufacturer of the vehicle equipped with automatic driving technologies, as well as by university institutes and public and private research bodies conducting experiments on vehicles equipped with driving automation technologies*. Cf. M. C. Gaeta, ‘Automazione e responsabilità civile automobilistica’ (2016) Responsabilità civile e previdenza 1717; A. Davola and R. Pardolesi, ‘In viaggio col robot: verso nuovi orizzonti della r.c. auto (“driverless”)’ (2017) 5 Danno e responsabilità 616; C. Severoni, ‘Prime considerazioni su un possibile inquadramento giuridico e sul regime di responsabilità nella conduzione dei veicoli a guida autonoma’ (2018) Diritto dei trasporti 356; D. Cerini, ‘Dal decreto “Smart Roads” in avanti: ridisegnare responsabilità e soluzioni assicurative’ (2018) Danno e responsabilità 4401; S. Scagliarini, ‘“Smart roads” e “driverless cars” nella legge di bilancio: opportunità e rischi di un’attività economica “indirizzata e coordinata a fini sociali”’ (2018) Quaderni costituzionali 497; C. Telesca, ‘Driverless cars: profili di responsabilità civile e penale’ (2019) Rivista di diritto della navigazione 183; S. Scagliarini, *Smart roads e driverless cars: tra diritto, tecnologie, etica pubblica* (Giappichelli 2019); S. Pollastrelli, *Driverless Cars: i nuovi confini della responsabilità civile automobilistica e prospettive di riforma*, in E. Calzolaio (ed.), *La decisione nel prisma dell’intelligenza artificiale* (Wolters Kluver 2020) 105; S. Pellegatta, ‘Autonomous Driving And Civil Liability: The Italian Perspective’ (2019) XVII Rivista di diritto dell’Economia, dei Trasporti e dell’Ambiente 135.

directly by a person or controlled remotely through advanced technological devices (levels three and four).[15]

As far as the concept of vehicle is concerned, in the first paragraph of Art. 46 of the Italian Traffic Code,[16] "vehicles" are defined as "all machines of any kind, circulating on the roads, driven by a person". The notion of vehicle, therefore, is inextricably linked to the presence of the human factor. This calls for further reflection: in order to try to guarantee new types of vehicles and, more generally, adequate protection for users, as it has already been done in German law, it is necessary to envisage legislative intervention to partially modify the aforementioned rule contained in the Italian Traffic Code.

What has just been highlighted appears to be closely linked also to the desire for a revision of the concept of driver, since it is also to be considered as such who, in the context of technological innovation in the entire sector, freely decides to activate the autonomous driving mode, remaining, however, always vigilant and ready to regain control of the vehicle if external circumstances or the computerised system should require it.[17]

In such a case an additional problem arises, namely that the driver of an automated vehicle will not easily be able to escape liability and to provide exonerating circumstances. For example, the data recorded by "black boxes"[18] could be useful in this respect, especially to check whether the vehicle was driven manually by a person or by computer devices at the time of the accident.

The Art. 2054 of the Italian Civil Code is the legal reference point for analysing liability for road traffic damages. This rule identifies a subjective criterion for attributing liability for alleged negligence to the driver, providing, verbatim, that "the driver of a vehicle that can circulate in traffic with freedom of choice of route is obliged to pay compensation for damage to people or property caused by the vehicle if the driver fails to prove that he or she did everything possible to avoid the damage".[19] This arrangement, also identifies, in the third paragraph, the joint

[15] In this regard, see A. Bertolini, 'Robot as products: the case for a realistic analysis of robotic applications and liability rules' (2013) Law, Innovation and Technology 214; Butti (n 1); Davola and Pardolesi (n 14); A Vedaschi and G. M. Noberasco, 'Gli autoveicoli a guida autonoma alla prova del diritto' (2019) Diritto pubblico comparato europeo 769.

[16] Legislative Decree No. 285 of 30 April 1992 "*Nuovo Codice della strada*", in *Gazzetta Ufficiale* No. 114, 18 May 1992, which came into force on 1 January 1993.

[17] Generally speaking, the driver is the person who takes over the direction of manoeuvres when driving a vehicle and their responsibilities. This assumption also refers to the contents of Art. 8 (Drivers) of the Vienna Convention of 8 November 1968 on traffic and road signs, ratified by the Italian Law No. 308 of 5 July 1995, in *Gazzetta Ufficiale* No. 174, 27 July 1995. The above-mentioned provision, in fact, provides that "Every moving vehicle or combination of vehicles shall have a driver. [...]. Every driver of a power-driven vehicle shall possess the knowledge and skill necessary for driving the vehicle; however, this requirement shall not be a bar to driving practice by learner-drivers in conformity with domestic legislation. Every driver shall at all times be able to control his vehicle [...]".

[18] They are mandatory data recording systems for highly or fully automated driving vehicles.

[19] To find out what many authors think, without in any way claiming to be exhaustive, see P. Trimarchi, *Rischio e responsabilità oggettiva* (Giuffrè 1961) 21; S. Rodotà, *Il problema della responsabilità civile* (Giuffrè 1964) 161 ff.; F. Galgano, *Trattato di diritto civile* (Wolters Kluwer 2015) III 230 ff.; F. Martini, 'L'obbligo assicurativo per la circolazione dei veicoli e dei natanti', in F. Martini and M. Rodolfi (eds), *Responsabilità da circolazione stradale* (Giuffrè 2018) 15 ff.; G. Alpa, *La responsabilità civile* (Giuffrè 2018) 472 ff.

responsibility of the owner of the vehicle, the usufructuary and the purchaser with a reserved dominion pact, who respond objectively, with the exception of situations for which they are able to demonstrate that the circulation has taken place against their will.[20]

With reference to the liability cases referred to in the Art. 2054 of the Italian Civil Code, the orientation of the judges of the Supreme Court of Cassation[21] was to consider the circulation of vehicles as a particular case of dangerous activity and, therefore, also from the point of view of liability, the Art. 2054 of the Italian Civil Code would be an application of the general principle contained in the Art. 2050 of the Italian Civil Code.[22]

A particularly important aspect to be assessed, in line with technological progress in the sector, is the identification of new responsible parties who will work alongside the driver and the vehicle owner. In this regard, it will be necessary to identify and regulate the responsibility of the manufacturer, which will be accompanied by that one of the supplier of the vehicle software, but also that one of the infrastructure, because if the accident is the result, for example, of programming defects or network malfunctions or other causes completely unrelated to the driver, the problem will arise of identifying which person or people is/are to be considered responsible.

Even though most reform projects developed in the sector are geared towards maintaining a subjective liability framework based on fault, it has been noted that the driver's focus on highly automated driving is lost in cases of fully autonomous driving.

The most widely held view according to many authors is that our regulatory system is based on the blame of a non-contractual liability of the person. This principle, if properly considered with the objective joint and several liability of the guarantee figures (owner, etc.) and the manufacturer/producer's liability could also remain valid for partially or totally connected and automated mobility systems.[23] This approach

[20] Cf. F. C. Barbarino, A. Franchina and S. Maci, *La responsabilità del produttore nella nuova disciplina* (Giuffrè 1989); R. Pardolesi, 'La responsabilità per danno da prodotti difettosi' (1989) Nuove leggi civili 497; A. Gorassini, *Contributo per un sistema della responsabilità del produttore* (Giuffrè 1990); G. Visintini, *Trattato breve della responsabilità civile* (Wolters Kluver 1996); G. Alpa and M. Bessone, *La responsabilità del produttore* (Giuffrè 1999); R. Scognamiglio, *Responsabilità civile e danno* (Giappichelli 2010).

[21] Cf. Supreme Court of Cassation (Joint Sessions), judgment of 29 April 2015, No. 8620; see S. Argine, 'Le Sezioni Unite e il concetto di circolazione stradale: luci ed ombre interpretative' (2016) Responsabilità civile e previdenza 214; A. Carrato, 'Le Sezioni unite chiariscono in via definitiva il concetto di "circolazione stradale" in funzione dell'operatività della disciplina della r.c.a.' (2015) 10 Il Corriere giuridico 1223; R. Pardolesi, 'Sul concetto di circolazione con riguardo al regime di assicurazione obbligatoria' (2015) 7-8 Foro italiano 2368. As a sign of conformity, it is also involved the Supreme Court of Cassation thanks to the Decree No. 25421 of 26 October 2017; see M. Marotta, 'Nella circolazione dei veicoli, in quanto attività pericolosa, è configurabile il caso fortuito' (2017) Diritto e Giustizia.

[22] Art. 2050 of the Italian Civil Code (Responsibility for the exercise of dangerous activities) provides that "anyone who causes damage to others in the performance of a dangerous activity, by its nature or by the nature of the means used, shall be liable to compensation, unless the person proves that he or she has taken all appropriate measures to avoid the damage". Cf. G. Mirabile, 'Le tendenze evolutive della giurisprudenza riguardo alla nozione di attività pericolosa' (2018) Responsabilità civile e previdenziale 454; L. Pari, 'Sulla configurabilità della navigazione aerea come attività pericolosa' (2018) Il Diritto marittimo 949.

[23] The concept of manufacturer includes both the car manufacturer that produces the vehicle and the company that takes care of the devices that are installed on board. With reference to the liability

should be supplemented, however, by a system based on the competitor's imputability of the guidance system supplier and/or software developer.

With a view to adapting to the changes that fully automated driving will bring to the entire transport system, a different perspective could be represented by identifying the figure of the manufacturer, as the person on whom liability for any accident caused by this category of vehicles should be directed.

In such situations, therefore, it would be desirable to introduce a "limited" strict liability system within which the producer can only be held liable if he or she does not comply with minimum safety standards.

4. *Concluding remarks*

In the face of rapid technological progress, the entire mobility system is facing multiple changes that are aimed at achieving greater safety for users in all modes of transport, reducing environmental impact by creating solutions based on sustainability, improving traffic flows through the implementation of information and digital technologies to achieve the ultimate goal of complete automation for vehicles.

Once the automation process is stabilised, it is assumed that the benefits will be multiple because innovative services to the community in terms of mobility will be guaranteed through public transport that is more flexible and closer to the needs of each user.

The experimentation of driving systems with a high level of automation, up to the total elimination of the driver, according to the estimates of some studies conducted at international level, should, among other things, provide for a drastic reduction in the number of accidents resulting from the circulation of vehicles, by about ninety percent compared to current parameters, as well as a significant reduction in carbon dioxide emissions into the air for a more profitable protection of the environment with a general economic saving estimated in the order of several billion dollars.

Environmental sustainability cannot, however, be assessed separately from economic parameters. For these reasons, encouraging sustainable mobility means implementing the private car sector alongside shared vehicles, as part of a broader system that makes it possible to connect driverless cars and smart cities, providing for a connection of the means of transport between them and with the infrastructure.

Mobility based on sustainable transport can only work if the whole system is adequate. This results into the need to build infrastructures and entire cities, the smart cities mentioned above, ready to welcome technological changes and to communicate with each other in a path of information exchange, connectivity, and simplification of urban viability.

regime, the manufacturer is liable, pursuant to Art. 114 of the Italian Legislative Decree No. 206 of 6 September 2005, the so-called *Codice del consumo* (Consumer's code), in *Gazzetta Ufficiale* No. 235, 8 October 2005, for damage caused by its defective products, but may provide proof of the facts that exclude its liability. The damaged party, on the other hand, is obliged to prove the defect, the damage and the causal link between defect and damage. The product can be considered defective, in general terms, if it lacks the minimum safety requirements and is dangerous for the people who use it and for third parties. Cf. Pardolesi (n 1); M. Bessone, 'La nozione di pericolo e il principio di responsabilità per i danni causati da attività pericolose' (1982) Rivista giuridica della circolazione e dei trasporti 855; M. Franzoni, *Dei fatti illeciti* (Giappichelli 1993) 491 ff.; Gaeta (n 14).

In order to proceed with the implementation of self-guided vehicles, in the near future, it will not be sufficient to adapt their technological equipment, but it will be necessary to foresee serious interventions on the existing infrastructures within the Italian territory and in the other countries of the European Union.

This is therefore a major challenge for Europe, where all States will have to work together to benefit from the development of automated road transport and they will also be able to compete with other countries such as China, Japan and the United States, which have already achieved excellent results in recent years.

In view of the expected benefits, however, it is impossible not to highlight how car manufacturers are revising the priorities and logic for the development of independent driving on vehicles because, according to data processed in the USA and disseminated in 2019 in the "Global Automotive Consumer Study", consumers have not yet gained the necessary confidence in self-driving vehicles and the most complex vehicles have high costs that are not justified by the perceived value.

A possible turning point could be to differentiate levels of self-driving according to the use of the vehicle and the environment in which it has to operate.

Specifically, levels from one (1) to three (3) could be dedicated to private customers while levels four (4) and five (5) could be dedicated to commercial uses such as autonomous shuttles and other on-demand mobility services, i.e. shared, operating in "simplified" environments such as urban centres with reduced costs borne by each user.

In conclusion, the legislator will have the task of regulating, in the more or less near future, the various aspects of road traffic, guaranteeing increasingly high levels of safety, in order to achieve an increasingly balanced mobility system aimed at protecting science, the economic interests of businesses, the fundamental rights of all citizens and environmental sustainability.

THE ETHICAL AND LEGAL IMPLICATIONS OF AUTONOMY IN WEAPONS SYSTEMS

DANIELE AMOROSO – GUGLIELMO TAMBURRINI

SUMMARY: 1. Introduction. – 2. Mapping the ethical and legal debate on AWS. – 3. Uniform policies for meaningful human control. – 4. The case for a prudential, differentiated and principled approach to meaningful human control. – 5. Concluding remarks.

1. *Introduction*

According to the most accredited view, to count as autonomous, a weapons system must be able to select and engage targets without any human intervention after its activation.[1] Starting from this basic and quite inclusive condition, the Stockholm International Peace Research Institute (SIPRI) introduced additional distinctions between types of existing Autonomous Weapons Systems (AWS):[2] (i) *air defense systems* (e.g. Phalanx[3]); (ii) *active protection systems*, which shield armoured vehicles by identifying and intercepting anti-tank missiles and rockets (e.g. Trophy[4]); (iii) *robotic sentries*, like the Super aEgis II stationary robotic platform tasked with the surveillance of the demilitarized zone between North and South Korea;[5] (iv) *guided munitions*, like the Dual-Mode Brimstone, which are endowed with the capability of autonomously identifying and engaging targets that are not in sight of the attacking aircraft;[6] (v) *loitering munitions*, such as the Harpy NG,[7] which overfly an assigned area in search of targets to dive-bomb and destroy.

This classification stands in need of continual expansion on account of ongoing military research projects on unmanned ground, aerial and marine vehicles that are capable of autonomously performing targeting decisions. Notably, research work based on swarm intelligence technologies is paving the way to swarms of small-size and low-

[1] Crucial stakeholders have converged around this formulation of central properties of "autonomy": one of the technologically most advanced military powers (US Department of Defense 'Autonomy in Weapons Systems' Directive 3000.09 (21 November 2012)), the main international humanitarian organization (International Committee of the Red Cross (ICRC), 'Views on autonomous weapon system' Paper submitted to the Informal meeting of experts on lethal autonomous weapons systems of the Convention on Certain Conventional Weapons (Geneva, 11 April 2016)), and the coalition of NGOs advocating a ban on AWS (Campaign to Stop Killer Robots, 'Urgent Action Needed to Ban Fully Autonomous Weapons' Press release (23 April 2013)).

[2] V. Boulanin and M. Verbruggen, *Mapping the Development of Autonomy in Weapon Systems* (SIPRI 2017).

[3] R. H. Stoner, 'R2D2 with Attitude: The Story of the Phalanx Close-In Weapons' (30 October 2009) NavWeap <www.navweaps.com/index_tech/tech-103.htm>.

[4] 'Trophy Active Protection System' (10 April 2007) Defense Update <https://defense-update.com/20070410_trophy-2.html>

[5] S. Parkin, 'Killer Robots: The soldiers that never sleep' (16 July 2015) BBC Future <www.bbc.com/future/story/20150715-killer-robots-the-soldiers-that-never-sleep>.

[6] UK Royal Air Force, *Aircraft & Weapons* (2007) 87.

[7] D. Gettinger and A. H. Michel, *Loitering Munitions* (Center for the Study of the Drone 2017).

cost unmanned weapons systems. These are expected to overwhelm enemy defenses by their numbers and may additionally perform autonomously targeting functions.[8]

The technological realities and prospects of AWS raise a major ethical and legal issue: Is it is permissible to let a robotic system unleash destructive force and take attendant life-or-death decisions without any human intervention? Public awareness about the ethical and legal implications of autonomous targeting had been raised by the Campaign "Stop Killer Robots", which was launched in 2013 by an international coalition of NGOs with the primary goal of "ban[ning] lethal robot weapons".[9] Worldwide pressures from civil society prompted States to initiate discussion of normative frameworks to govern the design, development, deployment and use of AWS. Diplomatic dialogues on this topic have been conducted since 2014 at the United Nations in Geneva, within the institutional framework of the Convention on Certain Conventional Weapons (CCW). Informal Meetings of Experts on lethal autonomous weapons systems were held on an annual basis at the CCW in Geneva, from 2014 to 2016. Subsequently, the CCW created a Group of Governmental Experts (GGE) on lethal autonomous weapons systems (LAWS), which still remains (as of 2020) the main institutional forum where the issue of autonomy in weapons systems is annually debated at an international level. Various members of the robotics research community take part to the GGE's meetings.[10] So far, the main outcome of the GGE's work is the adoption by consensus of a non-binding instrument, that is, the 11 Guiding Principles on LAWS.[11]

An examination of the Guiding Principles, and more in general of the debate at the GGE, shows that discussions on AWS have been progressively zooming in on distinctive roles for the "human element" to play in the use of force. Indeed, it is widely agreed on by participants in these debates that the identification of normatively acceptable human-weapon interactions constitutes the keystone of any future regulation of AWS. Both the Campaign and an increasing number of States have come to maintain that a requirement should be established under international law, to rule that any weapons systems must be subject to meaningful human control (MHC).[12] It is exactly here, however, that international consensus stops. Indeed, it is far from settled – even among those favoring an MHC requirement – what its actual content should be or, to put it more sharply, what is normatively demanded to make human control over weapon systems truly "meaningful".

[8] See, among many others, P. Scharre, *Robotics on the Battlefield Part II. The Coming Swarm* (Center for a New American Security, October 2014) and M. Brehm and A. de Courcy Wheele, 'Swarms' Article36 discussion paper for the Convention on Certain Conventional Weapons (Geneva, March 2019).

[9] Campaign to Stop Killer Robots (n 1).

[10] More information on these meetings are available on the webpage of the UN Office at Geneva: <https://unog.ch>.

[11] High Contracting Parties to the Convention on Conventional Weapons, 'Final Report of the 2019 Meeting' (13 December 2019) UN Doc CCW/MSP/2019/CRP.2/Rev.1, Annex III ("Guiding Principles on Lethal AWS").

[12] The MHC formula made its first appearance in the AWS debate in a 2013 paper by the UK-based NGO Article 36 (*Killer Robots: UK Government Policy on Fully Autonomous Weapons* (Article 36, April 2013) <http://www.article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf>. For a survey of the States supporting the MHC requirement, see Human Rights Watch, *Stopping Killer Robots Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control* (August 2020).

Against this background, this contribution is aimed to provide an overview of the AWS debate, with a focus on the MHC turning point and its ethical and legal underpinnings. In Section 2 a schematic account is provided of chief ethical and legal concerns about autonomy in weapons systems. Then, the main proposals regarding the MHC content are introduced and analyzed, including our own proposal of a "principled, differentiated and prudential" human control policy on AWS. Finally, it is pointed out how our proposal may help overcome the hurdles that are currently preventing the international community from adopting a legal regulation on the matter.

2. *Mapping the ethical and legal debate on AWS*

A clear outline of the main ethical and legal concerns raised by AWS is found already in a 2013 Report, significantly devoted to "lethal autonomous robotics and the protection of life", by the UN Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns.[13] These concerns are profitably grouped under four headings: (i) *compliance with IHL*, (ii) *responsibility ascription problems*, (iii) *violations of human dignity*, and (iv) *increased risk for peace and international stability*. Let us briefly expand on each one of them, by reference to relevant sections in Heyns' report.

(i) Compliance with IHL would require capabilities that are presently possessed by humans only, and that no robot is likely to possess in the near future, i.e., to achieve situational awareness in unstructured warfare scenarios and to formulate appropriate judgments there (paras. 63-74);[14]

(ii) Autonomy in weapons systems would hinder responsibility ascriptions in case of wrongdoings, by removing human operators from the decision-making process (paras. 75-81);[15]

(iii) The deployment of lethal AWS would be an affront to human dignity, which dictates that decisions entailing human life deprivation should be reserved to humans (paras. 89-97);[16]

(iv) Autonomy in weapons systems would threaten in special ways international peace and stability, by making wars easier to wage on account of reduced numbers of involved soldiers, by laying the conditions for unpredictable

[13] 'Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions' UN Doc. A/HRC/23/47, 9 April 2013

[14] For a critique to this argument, see M. N. Schmitt and J. S. Thurnher, '"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict' (2013) 4 Harvard National Security Journal 231; M. Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 International Law Studies 308. See also, for a convincing rejoinder, T. Krupiy, 'Of Souls, Spirits and Ghosts: Transposing the Application of the Rules of Targeting to Lethal Autonomous Robots' (2015) 16 Melbourne Journal of International Law 145.

[15] For further discussion, see Carrie McDougall, 'Autonomous Weapon Systems and Accountability: Putting the Cart before the Horse' (2019) 20 Melbourne J of Intl L 58.

[16] For an overview of the debate on this issue, see Daniele Amoroso, *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains* (ESI/Nomos 2020), 161-215.

interactions between AWS and their harmful outcomes, by accelerating the pace of war beyond human reactive abilities (paras. 57-62).[17]

These sources of concern jointly make the case for claiming that a meaningful human control (MHC) over weapons systems should be retained exactly in the way of their critical target selection and engagement functions. Accordingly, the notion of MHC enters the debate on AWS as an ethically and legally motivated constraint on the use of any weapons systems, including autonomous ones. The issue of human-robot shared control in warfare is thereby addressed from a distinctive humanitarian perspective, insofar as autonomous targeting may impinge, and deeply so, upon the interests of persons and groups of persons that are worthy of protection from ethical or legal standpoints.

But what does MHC more precisely entail? What is normatively demanded to make human control over weapon systems truly "meaningful"? The current debate about AWS, which we now turn to consider, is chiefly aimed to provide an answer to these questions.

3. *Uniform policies for meaningful human control*

The foregoing ethical and legal reasons go a long way towards shaping the content of MHC, by pinpointing general functions that should be prescriptively assigned to humans in shared control regimes, and by providing general criteria to distinguish perfunctory from truly meaningful human control. More specifically, the ethical and legal reasons for MHC suggest a threefold role for human control on weapon systems to be "meaningful". First, the obligation to comply with IHL entails that human control must play the role of a *fail-safe actor*, contributing to prevent a malfunctioning of the weapon from resulting in a direct attack against the civilian population, or in excessive collateral damages.[18] Second, in order to avoid accountability gaps, human control is required to function as *accountability attractor*, i.e. to secure the legal conditions for responsibility ascription in case a weapon follows a course of action that is in breach of international law.[19] Third and finally, from the principle of human dignity respect it follows that human control should operate as a *moral agency enactor*, by ensuring that decisions affecting the life, physical integrity and property of people (including combatants) involved in armed conflicts are not taken by non-moral artificial agents.[20]

But how are human-weapon partnerships to be more precisely shaped on the basis of these broad constraints? Several attempts to answer this question have been made by parties involved in the AWS ethical and legal debate. The answers that we turn to examine now outline *uniform* human control policies, whereby one size of human

[17] On this issue, see J. Altmann and F. Sauer, 'Autonomous Weapon Systems and Strategic Stability' (2017) 59 Survival 117-142.

[18] P. Scharre, 'Centaur Warfighting: The False Choice of Humans v. Automation' (2016) 30 Temple International and Comparative Law Journal 151, 154.

[19] Th. Chengeta, 'Defining the emerging notion of "Meaningful Human Control" in autonomous weapon systems' (2017) 49 New York Journal of International Law and Politics 833, 888.

[20] ICRC, 'Ethics and autonomous weapon systems: An ethical basis for human control?' Working paper submitted to the Group of Governmental Experts on lethal autonomous weapons of the Convention on Conventional Weapons (Geneva, 29 March 2018) UN Doc CCW/GGE.1/2018/WP.5.

control is claimed to fit all AWS and each one of their possible uses. These are the "boxed autonomy", "denied autonomy" and "supervised autonomy" control policies.

The boxed autonomy policy assigns to humans the role of constraining the autonomy of a weapons system within an operational box, constituted by "predefined [target] parameters, a fixed time period and geographical borders".[21] Accordingly, the weapons system would be enabled to autonomously perform the critical functions of selecting and engaging targets, but only within the boundaries set forth by the human operator or the commander at the planning and activation stages.[22]

The boxed autonomy policy seems to befit a variety of *deliberate targeting* situations, which involve military objectives that human operators know in advance and can map with high confidence within a defined operational theatre. It seems, however, unsuitable to govern a variety of *dynamic targeting* situations. These require one to make changes on the fly to planned objectives and to pursue targets of opportunity. The latter are unknown to exist in advance (unanticipated targets) or else are not localizable in advance with sufficient precision in the operational area (unplanned targets). Under these conditions, boxed autonomy appears to be problematic from a normative perspective, insofar issues of distinction and proportionality that one cannot foresee at the activation stage may arise during mission execution.

By the same token, a boxed autonomy policy may not even suffice to govern deliberate targeting of military objectives placed in unstructured warfare scenarios. To illustrate, consider the loitering munition Harpy NG, which is endowed with the capability of patrolling for several hours a predefined box in search of enemy targets satisfying given parameters. The conditions licensing the activation of this loitering munition may become superseded if civilians enter the boxed area, erratic changes occur or surprise-seeking intentional behaviors are enacted.[23] Under these various circumstances, there is "fail-safe" work for human control to do at the mission execution stage too.

In sharp contrast with the boxed autonomy policy, the denied autonomy policy rules out any autonomy whatsoever for weapons systems in the critical targeting function, and therefore embodies a most restrictive interpretation of MHC.[24] Denied autonomy undoubtedly fulfils the threefold normative role for human control as fail-safe actor, accountability attractor, and moral agency enactor. However, this policy has been sensibly criticized for setting too high a threshold for machine autonomy, in ways that are divorced from "the reality of warfare and the weapons that have long been

[21] International Panel on the Regulation of Autonomous Weapons (IPRAW), *Focus on Human Control* (August 2019).

[22] This solution is advocated by the Dutch government, which endorsed on this point the recommendations issued by the Dutch Advisory Council on International Affairs (AIV) and Advisory Committee on Issues of Public International Law (CAVV) in their joint report 'Autonomous weapon systems: the need for meaningful human control' (2015) No. 97 AIV / No. 26 CAVV. For a more detailed account of this approach, see M. Roorda, 'NATO's Targeting Process: Ensuring Human Control Over and Lawful Use of 'Autonomous' Weapons', in A. Williams and P. Scharre (eds), *Autonomous Systems: Issues for Defence Policymakers* (NATO, 2015) 152; M. A. C. Ekelhof, 'Moving Beyond Semantics on Autonomous Weapons Systems: Meaningful Human Control in Operation' (2019) 10 Global Policy 343.

[23] D. Akerson, 'The Illegality of Offensive Lethal Autonomy', in D. Saxon (ed.), *International Humanitarian Law and the Changing Technology of War* (Brill/Nijhoff, 2013) 65, 87.

[24] Chengeta (n 19).

considered acceptable in conducting it."[25] To illustrate this criticism, consider air defensive systems, which autonomously detect, track, and target incoming projectiles. These systems have been aptly classified as SARMO weapons, where SARMO stands for "Sense and React to Military Objects". SARMO systems are hardly problematic from ethical and legal perspectives, in that "they are programmed to automatically perform a small set of defined actions repeatedly. They are used in highly structured and predictable environments that are relatively uncluttered with a very low risk of civilian harm. They are fixed base, even on Naval vessels, and have constant vigilant human evaluation and monitoring for rapid shutdown".[26]

SARMO systems expose the overly restrictive character of a denied autonomy policy. Thus, one wonders whether milder forms of human control might be equally able to strip the autonomy of weapons systems of its ethically and legally troubling implications. This is indeed the aim of the supervised autonomy policy, which occupies a middle ground between boxed and denied autonomy, insofar as it requires humans to be on-the-loop of AWS missions.

As defined in the US DoD Directive 3000.09 on "Autonomy in Weapons Systems", human-supervised AWS are designed "to provide human operators with the ability to intervene and terminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur".[27] Notably, human-supervised AWS may be used for defending manned installations and platforms from "attempted time-critical or saturation attacks", provided that they do not select "humans as targets" (see, e.g., the Phalanx Close-In Weapons System in use on US surface combat ships).[28] While undoubtedly effective for these and other warfare scenarios, supervised autonomy is not the silver bullet for every ethical and legal concern raised by AWS. To begin with, by keeping humans on-the-loop one would not prevent faster and faster offensive AWS from being developed, eventually reducing the role of human operators to a perfunctory supervision of decisions taken at superhuman speed, while leaving the illusion that the human control requirement is still complied with.[29] Moreover, the automation bias – the human propensity to overtrust machine decision-making processes and outcomes – is demonstrably exacerbated by a distribution of control privileges that entrusts humans solely with the power of overriding decisions autonomously taken by the machines.[30]

To sum up. Each one of the boxed, denied, and supervised autonomy policies provides useful hints towards a normatively adequate human-machine shared control policy for military target selection and engagement. However, the complementary defects of these *uniform* control policies suggest the implausibility of solving the MHC problem with one formula, to be applied to all kinds of weapons systems and to each one of their possible uses. This point was consistently made by the US delegation at

[25] M. C. Horowitz and P. Scharre, *Meaningful Human Control in Weapon Systems: A Primer* (Center for a New American Security, March 2015).

[26] International Committee for Robot Arms Control, 'Statement on technical issues' delivered at the informal meeting of experts on lethal autonomous weapons (Geneva, 14 May 2014).

[27] US DoD Directive (n. 1), 13.

[28] Ibid., 3 para. 4(c)(2).

[29] E. Schwarz, 'The (Im)possibility of Meaningful Human Control for Lethal Autonomous Weapon Systems' (29 August 2018) Humanitarian Law & Policy <https://blogs.icrc.org/law-and-policy/2018/08/29/im-possibility-meaningful-human-control-lethal-autonomous-weapon-systems/>.

[30] L. J. Skitka, K. L. Mosier and M. Burdick, 'Does Automation Bias Decision-making?' (1999) 51 International Journal of Human-Computer Studies 991.

GGE meetings in Geneva: "there is not a fixed, one-size-fits-all level of human judgment that should be applied to every context".[31]

4. *The case for a prudential, differentiated and principled approach to meaningful human control*

Other approaches to MHC aim to reconcile the need for differentiated policies with the above ethical and legal constraints on human control. Differentiated policies modulate human control along various autonomy levels for weapons systems. A taxonomy of increasing autonomy levels concerning the AWS critical target selection and engagement functions was proposed by Noel Sharkey (and only slightly modified here, with regard to levels 4 and 5):[32]

L1. A human engages with and selects targets and initiates any attack.

L2. A program suggests alternative targets and a human chooses which to attack.

L3. A program selects targets, and a human must approve before the attack.

L4. A program selects and engages targets but is supervised by a human who retains the power to override its choices and abort the attack.

L5: A program selects targets and initiates attack on the basis of the mission goals as defined at the planning/activation stage, without further human involvement.

The main uniform control policies, including those examined in the previous section, are readily mapped onto one of these levels.

(L5) corresponds to the boxed autonomy policy, whereby MHC is exerted by human commanders at the planning stage of the targeting process only. As noted above, boxed autonomy does not constitute a sufficiently comprehensive and normatively acceptable form of human-machine shared control policy.

(L4) corresponds to the supervised autonomy policy. The uniform adoption of this level of human control must also be advised against, in the light of automation bias risks and increasing marginalization of human oversight. In certain operational conditions, however, it may constitute a normatively acceptable level of human control.

(L3) has been seldom discussed in the MHC debate. At this level, control privileges on critical targeting functions are equally distributed between weapon system (target selection) and human operator (target engagement). To the extent that the human deliberative role is limited to approving or rejecting targeting decisions suggested by the machine, this level of human control does not provide adequate bulwarks against the risk of automation bias.[33] In the same way as (L4), therefore, it should not be adopted as a general policy.

(L1) and (L2) correspond to shared control policies where the weapons system's autonomy is either totally absent (L1) or limited to the role of adviser and decision support system for human deliberation (L2). The adoption of these pervasive forms of

[31] United States, 'Human-Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems' Working paper submitted to the Group of Governmental Experts on lethal autonomous weapons of the Convention on Conventional Weapons (Geneva, 28 August 2018) UN Doc CCW/GGE.2/2018/WP.4.

[32] N. E. Sharkey, 'Staying the Loop: Human Supervisory Control of Weapons', in N. Bhuta et al. (eds), *Autonomous Weapons Systems. Law, Ethics, Policy* (CUP, 2016) 23, 34-37.

[33] M. L. Cummings, 'Automation and Accountability in Decision Support System Interface Design' (2006) The Journal of Technology Studies 23.

human control must also be advised against, insofar as some weapons (notably SARMO systems) have long been considered acceptable in warfare operations.

In the light of these difficulties, one might be tempted to conclude that the search for a comprehensive and normatively binding MHC policy should be given up, and that the best one can hope for is the exchange of good practices between States about AWS control, in addition to the proper application of national mechanisms to review the legality of weapons.[34] But alternatives are possible, which salvage the idea of a comprehensive MHC policy, without neglecting the need for differentiated levels of AWS autonomy in special cases. Indeed, the authors of this contribution have advanced the proposal of a comprehensive MHC policy, which is jointly *prudential*, *differentiated* and *principled*.[35]

The *prudential* character of this policy is embodied into the following default rule: high levels of human control L1-L2 should be exerted on all weapons systems and uses thereof, unless the latter are included in a list of exceptions agreed on by the international community of States. The prudential imposition by default of L1 and L2 is aimed at minimizing the risk of breaches of IHL, accountability gaps, or affronts to human dignity, should international consensus be lacking on whether, in relation to certain classes of weapons systems or uses thereof, higher levels of machine autonomy are equally able to grant the fulfilment of genuinely meaningful human control. The *differentiated* character of this policy is embodied in the possibility of introducing internationally agreed exceptions to the default rule. However, these exceptions should come with the indication of what level is required to ensure that the threefold role of MHC (fail-safe actor, accountability attractor, moral agency enactor) is adequately performed, which characterizes our approach as *principled*.

In the light of the above analysis, this should be done by taking into account at least the following observations:

a) The (L4) human supervision and veto level might be deemed as an acceptable level of control only in case of anti-materiel AWS with exclusively defensive functions (e.g. Phalanx or Iron Dome). In this case, ensuring that human operators have full control over every single targeting decision would pose a serious security risk, which makes the application of (L1), (L2), and (L3) problematic from both military and humanitarian perspectives. The same applies to active protection systems, like Trophy, provided that their use in supervised-autonomy mode is excluded in operational environments involving a high concentration of civilians.

b) (L1) and (L2) could also be impracticable in relation to certain missions because communication constraints would allow only limited bandwidth. In this case,

[34] See, e.g., the views expressed by Switzerland ('A "compliance-based" approach to Autonomous Weapon Systems' Working paper submitted to the Group of Governmental Experts on lethal autonomous weapons of the Convention on Conventional Weapons (Geneva, 10 November 2017) UN Doc CCW/GGE.1/2017/WP.9) and United States ('Statement for the General Exchange of Views' delivered at the Group of Governmental Experts on lethal autonomous weapons of the CCW (Geneva, 9 April 2018).

[35] For an early exposition of this approach, see Daniele Amoroso and Guglielmo Tamburrini. *What Makes Human Control over Weapon Systems "Meaningful"?* (International Committee for Robot Arms Control, August 2019). See also V. Boulanin et al., *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control* (June 2020) SIPRI <https://www.sipri.org/sites/default/files/2020-06/2006_limits_of_autonomy_0.pdf>.

military considerations should be balanced against humanitarian ones. One might allow for less bandwidth-heavy (L3) control in two cases: deliberate targeting and dynamic targeting in fully structured scenarios, e.g. in high seas. In both hypotheses, indeed, the core targeting decisions have actually been taken by humans at the planning/activation stage. Unlike (L4), however, (L3) ensures that there is a human on the attacking end who can verify, in order to deny or grant approval, whether there have been changes in the battlespace which may affect the lawfulness of the operation. Looking at existing technologies, (L3) might be applied to sentry robots deployed in a fully structured environment, like the South-Korean Super aEgis II.

c) The (L5) boxed autonomy level should be considered incompatible with the MHC requirement, unless operational space and time frames are so strictly circumscribed to make targeting decisions entirely and reliably traceable to human operators.

5. *Concluding remarks*

Recent advances in autonomous military robotics have raised unprecedented ethical and legal issues. Regrettably, diplomatic discussions at the GGE in Geneva not only have so far fallen short of working out a veritable legal regime on meaningful human control over AWS, but – what is worse – are currently facing a stalemate, which is mainly determined by the opposition of major military powers, including the US and the Russian Federation, to the adoption of any kind of international regulation on the matter.[36]

Our proposal of relinquishing the quest for a one-size-fits-all solution to the MHC issue in favour of a suitably differentiated approach may help sidestep current stumbling blocks. Diplomatic and political discontent about an MHC requirement that is overly restrictive with respect to the limited autonomy of some weapons systems might indeed be mitigated recognising the possibility of negotiating exceptions to L1-L2 human control, by identifying weapons systems and contexts of use where milder forms of human control will suffice to ensure the fulfilment of the fail-safe, accountability, and moral agency properties whose preservation generally underpins the normative concerns about weapons' autonomy in targeting critical functions.

[36] D Lewis, 'An Enduring Impasse on Autonomous Weapons' (28 September 2020) Just Security <https://www.justsecurity.org/72610/an-enduring-impasse-on-autonomous-weapons>.

PART III

ARTIFICIAL INTELLIGENCE AND SMART CITIES

INTRODUCTION

ALESSIO BARTOLACELLI – CHIARA FELIZIANI – FRANCESCA SPIGARELLI

"Smart city" is a wording that has been in vogue for some years and in different contexts. It is present, in fact, in the narrative related to many international and European policy documents or legal texts, as well as in academic essays belonging to different disciplines, or in more colloquial environments.

Confirmed by the broad use of the expression, "smart city" is a wording which has multiple meanings, or it can refer to different aspects of the cities' life. That is mainly because more elements combine to make smart a city. Urban planning, transport system, social inclusion policies are just some of the aspects that compete in doing so. Indeed, digital and telecommunication technologies play a growing and relevant role in the context of cities and, above all, in the smart management and regulation of them. This has become even more clear after the advent of the COVID-19 pandemic.

The contribution of new technologies within the context of smart cities is explicitly recognised by important international documents, such as the New Urban Agenda (UN Doc. A/71/256, 25 January 2017) and the 2030 Agenda for Sustainable Development (UN Doc. A/RES/70/1, 21 October 2015). Technologies are considered a fundamental tool to reach in a more effective and efficient way the above-mentioned goals. Technologies can also guarantee a smart regulation of cities in their several aspects: energy supply, transports, health services and so on.

In this context, this section of the book is devoted to exploring with a multidisciplinary approach, some applications of new technologies and artificial intelligence to different relevant aspects of the city life, for the benefit of its inhabitants and business.

In the first paper, E. Frontoni and L. Romeo underline that "the AI algorithm may provide an affordable solution to support cities to become self-regulated by exploring cities as real-time, living dynamics systems and overcoming the challenges" related to – for example – energy saving, traffic congestion, ageing population and health.

Again from an engineering perspective, the paper written by A. Arteconi is focused on the process of Energy Transition. Moving from the assumption that "the present energy scenario is characterized by an increasing penetration of renewable energy sources (RES)" and that such a penetration "introduces uncertainty in the available production capacity", the essay describes the features and the potentialities of the Electric Smart Grid in guaranteeing the efficiency of the energy supply.

The paper of G. Menegus focuses the attention on the legal implications of technologies applied to services within the cities. It analyses "the concept of regulatory intermediation in its applications to home-sharing platforms". In doing so, the essay focuses on two case studies, i.e. the French 120-day cap and the Italian local agreement for the tourist tax collection, and underlines lights and shadows of these platforms.

Finally, the contribution by M. Paroli takes into consideration the impact of technological innovation and AI on intermodal transport, with a specific focus on a case study in the Port of Ancona. In particular, the paper considers the interaction between the TinS (Secure transfer) project with an AI technology (A3iu software) to allow an autonomous identification of people and vehicles in the Port of Ancona. Such implementation sees the cooperation between the Port Authority, Customs Agency and Customs Police, optimising the overall efficiency of the entire Port infrastructure.

ARTIFICIAL INTELLIGENCE APPLIED TO CITIES

EMANUELE FRONTONI – LUCA ROMEO

SUMMARY: 1. The mission of AI. – 1.2. Ethical AI guidelines. – 2.2. Decision Support System. – 2. Smart Cities. – 2.1. Definition. – 2.2. Smart City areas and challenges. – 3. Smart Cities and Artificial Intelligence. – 3.1. How Smart Cities are using Artificial Intelligence. – 3.2. Advanced Security Camera & Surveillance System. – 3.3. Benefits and Challenges.

1. *The mission of AI*

The design, development and application of Artificial Intelligence (AI) technologies should foresee the verification of reliability (ethicality) of the overall system and of all processes in the specific context.[1] In order to ensure ethicality, the following requirements must be ensured, which must be continuously assessed throughout the entire cycle of the AI system: a) human agency and oversight, b) technical robustness and safety, c) privacy and data governance, d) transparency, e) diversity, non-discrimination and fairness, f) societal and environmental well-being, g) accountability.[2]

1.1. *Ethical AI Guidelines*

The ML/DL algorithm should ensure a high robustness and safety against adversarial attacks, poisoning attacks, model theft and model and data privacy. The adversarial samples may lead to various misbehaviors of the model, that can be erroneously positively perceived by humans. The adversarial robustness should be ensured by including solutions for detecting adversarial samples, for evaluating the sensibility of the model against adversarial attacks, for ensuring a robust model architecture. At the same time, a tempestively detection of poisoning attacks during the inference time can avoid backdoors and the degradation of performance. The overall architecture that encapsulates the AI model should be conceived to detect and prevent model theft via API.

To ensure provable privacy guarantees for training data, secure federate learning based on blockchain strategies should be taken into account to build a ML model which learns from distributed training datasets while providing privacy preservation and immunity to adversarial attacks.

The legal principle of data minimization should be respected by using only relevant personal data that are adequate and limited to what is necessary for the purpose pursued (Art. 5 GDPR) and the need to anonymize, pseudonymize, encrypt personal health data according to the specific context (Articles 6 and 25 GDPR).

[1] High-Level Expert Group on AI, *Ethics guidelines for trustworthy AI*, 8 April 2019 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419>; European Commission, *White Paper - On Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final, 19 February 2020.

[2] Ibid., Chapter II, 58.

Explainability and transparency are two key factors of the AI system that should be ensured during the design process. An explainable or interpretable ML/DL model is not limited to answer the pattern discrimination question (e.g. predict the pathology using the electronic health record information data) but it is also able to carry out the pattern localization and pattern characterization questions. In fact, once it has been predicted that a specific patient has a certain risk of contracting a pathology, it may be clinically relevant to go ahead by answering where and how this discriminatory information is encoded (e.g. detecting the most discriminative predictors that contribute most to the prediction of the model. Starting from a growing demand for explainable AI ranging from Industry[3] and Health scenarios,[4] the proposing of interpretability and explanation methods for gaining a better understanding about the decision rule and the problem-solving abilities of high nonlinear models (DL) are therefore receiving increased attention in the ML community. There are usually three dimensions of explainability including (i) models that are directly interpretable rather than a post hoc interpretation, (ii) model-level interpretability rather than instance-level interpretability and (iii) static or interactive interpretability.

Additionally, the transparency requirement ensures that the outcome of the AI system is explained in a comprehensive manner adapted to the stakeholder involved. This fact implies that the model should match the complexity capability and the domain knowledge of the consumer.

The ML/DL model should guarantee the fairness and non-discrimination principle. The model should not lead to any prejudice for or against something. However, the ML model learns on data collected by humans and humans for their nature are biased. Additionally, the ML model is conceived to learn from examples and generalizing to situations never seen before.

The bias detection and mitigation strategies should be embedded in the system in order to avoid unfair and/or unwanted bias that may lead to having negative implications such as the marginalization of vulnerable groups. However, often the lack of common-sense knowledge, the lack of representative data and the goal / values not well defined may lead to a situation where the AI agents do unexpected and undesired actions. Solutions that overcome this issue may involve the introduction of ethical constraints in a recommender system or the integration of both preferences and ethical priorities in the ML algorithm or in the AI framework.

[3] L. Romeo, J. Loncarski, M., Paolanti, G. Bocchini, A. Mancini and E. Frontoni, 'Machine learning-based design support system for the prediction of heterogeneous machine parameters in industry 4.0.' (2020) 140 Expert Systems with Applications 112869.

[4] M. Bernardini, M. Morettini, L. Romeo, E. Frontoni and L. Burattini, 'Early temporal prediction of Type 2 Diabetes Risk Condition from a General Practitioner Electronic Health Record: A Multiple Instance Boosting Approach' (2020) 105 Artificial Intelligence in Medicine 101847; M. Bernardini, L. Romeo, P. Misericordia and E. Frontoni, 'Discovering the Type 2 Diabetes in Electronic Health Records Using the Sparse Balanced Support Vector Machine" (2020) 24 IEEE Journal of Biomedical and Health Informatics 235; L. Romeo, G. Armentano, A. Nicolucci, M. Vespasiani, G. Vespasiani and E. Frontoni, 'A Novel Spatio-Temporal Multi-Task Approach for the Prediction of Diabetes-Related Complication: a Cardiopathy Case of Study', in *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence Special track on AI for CompSust and Human well-being*, 2020, 4299 ff.

The principle of accountability plays a central role, especially in critical applications such as the capital market[5] and clinical scenario.[6]

The assessment of the outcome is clearly provided for each processing and algorithm step: the user/customers should be able to actively interact with the AI model, ensuring that the objectives are achieved.

These guidelines are the foundations that are taken into account in the design of the AI system that is from one side able to provide support of the human decisions and at the same time is put in the condition to provide significant benefit to human beings.

1.2. *Decision Support System*

The AI system should support the human behind their decision-making processes and corresponding actions. This fact implies to empower human beings, allowing them to make informed and valuable decisions.

Hence, the mission is not limited to research and development from a theoretical perspective a novel machine learning (ML) or deep learning (DL) algorithm, but a crucial role is ensured by the integration of the algorithm in a decision support system (DSS). Examples of DSS based on ML algorithm range and are not limited to Industry 4.0, eHealth, Social Media Intelligence,[7] consumer behavior[8] and capital market. Additionally, these approaches should take into account proper oversight of human-computer interaction mechanisms based on human-in-the-loop, human-on-the-loop and human-in-command strategies. In the human-in-the-loop approach, humans are involved to annotate data in order to feed a ML model with high quality and high quantities of training data. After the ML algorithm learns the decision rule to solve a specific task from this data, the human is responsible to tune the model (e.g. modifying hyperparameters of the model to alleviate overfitting). It is worth mentioning here that each of these actions comprises a continuous feedback loop in order to improve the generalization power of the model. At the same time, a human-in-command approach is requested to maintain the human's supervision of the algorithm and the machine, by choosing when and where we want that certain tasks (e.g. medical decisions) are carried out by AI.

2. *Smart Cities*

The smart city is a fluid, friendly, connected, intelligent and simple city. It includes different thematic areas such as smart health, smart education, smart building smart mobility and smart government. These areas are interconnected by mobile wireless and fixed broadband technology.

[5] R. Rosati, L. Romeo, C. A. Goday, T. Menga and E. Frontoni, 'Machine Learning in Capital Markets: Decision Support System for Outcome Analysis' (2020) 8 IEEE Access 109080.

[6] See *supra* (n. 3, 4 and 5).

[7] M. Paolanti, C. Kaiser, R. Schallner, E. Frontoni and P. Zingaretti, 'Visual and textual sentiment analysis of brand-related social media pictures using deep convolutional neural networks', in *International Conference on Image Analysis and Processing* (Springer 2017) 402 ff.

[8] M. Paolanti, D. Liciotti, R. Pietrini, A. Mancini and E. Frontoni, 'Modelling and forecasting customer navigation in intelligent retail environments' (2018) 91 Journal of Intelligent & Robotic Systems 165; M. Paolanti, L. Romeo, M. Martini, A. Mancini, E. Frontoni and P. Zingaretti, 'Robotic retail surveying by deep learning visual and textual data' (2019) 118 Robotics and Autonomous Systems 179.

2.1. *Definition*

A smart city connects human capital, social capital and Information and Communication Technologies (ICT) infrastructure in order to address public issues, achieve sustainable development and increase the quality of life of its citizens. The smart city goals can be summarized as follows:

- Achieve sustainable development.
- Increase the quality of life of its citizens.
- Improve the efficiency of the existing and new infrastructures.

ICT is a tool for the improvement of the city by ensuring the achievement of the above-mentioned objectives.

The main actors can be defined as (i) government and city authorities (ii) public-private partnerships and (iii) Citizen participation. The scope of the smart city is focused on the economic and social expansion of the whole region, the connected settlements, and the improvement to the regional and interregional networks.

2.2. *Smart city areas and challenges*

Tab. 1 summarizes the smart city areas in terms of action fields which range from governance, economy, mobility, environment, people, living.

Sustainable City Aspects	**City Axes**	**Smart City Action Fields**	**Smart City Areas**
Economic	Institutions	Governance	Participation
			Transparency
			Public and social services
		Economy	Innovation
			Entrepreneurship
Environmental	Habitat	Mobility	Traffic
			Public Transport
			ICT Infrastructure
			Logistics
		Environment	Network and environmental monitoring
			Energy efficiency
Social	Citizen	People	Digital education
			Creativity
		Living	Tourism & culture
			Health & safety
			Technology accessibility

Tab 1: Smart city action fields and areas

For each smart city action field, we report in Tab. 2 the related smart city challenges. Examples of various types of issues in the cities are proactive maintenance, prioritization of work, infrastructure condition assessment, damaged roads and buildings, blind spots on assets, maintenance cost optimization.

The employment of Artificial Intelligence (AI) approaches may empower the ICT tools to overcome the reported challenges.

Governance	Economy	Mobility	Environment	People	Living
Flexible governance	Unemployment	Sustainable mobility	Energy saving	Unemployment	Affordable housing
Shrinking cities	Shrinking cities	Inclusive mobility	Shrinking cities	Social cohesion	Social cohesion
Combination of formal and informal government	Economic decline	Multimodal public transport system	Holistic approach to environmental and energy issues	Poverty	Health problems
Territorial cohesion	Territorial cohesion	Pollution	Pollution	Ageing population	Crime rate
	Mono-sectorial economy	Traffic congestion	Urban sprawl	Social diversity as source of innovation	Urban sprawl
	Sustainable local economies	Non-car mobility			
	Social diversity as source of innovation				

Tab 2: Smart city challenges

3. *Smart Cities and Artificial Intelligence*

The recent advance in AI and the increasing amount of available data move us closer to developing an urban operating system that simulates human, machine, and environmental patterns[9]. Thus, the AI algorithm may provide an affordable solution to support cities to become self-regulated by exploring cities as real-time, living, dynamics systems and overcoming the challenges reported in Tab. 2. Smart Cities and AI brings together a multidisciplinary, integrated approach related of how the combination of human and machine intelligence is transforming the experience of the urban environment.[10]

3.1. *How Smart Cities are using Artificial Intelligence*

There are different examples on how AI and ML can play a crucial role to solve the above-mentioned challenges (see Tab. 2).

Below some examples of AI initiatives are reported for each smart city action field.

- Governance: Better governance and planning management[11] – AI and ML techniques may be used to map land use across time to generate crucial insights using the satellite imagery and aerial view 2D or 3D images of geographical areas. The trained ML algorithm can analyze satellite images for city planning and development with scope to adjust the formation based on calamities like flooding,

[9] Ch. G. Kirwan and Zh. Fu, *Smart Cities and Artificial Intelligence* (Elsevier 2020) ii.

[10] Paolanti, Romeo, Martini, Mancini, Frontoni and Zingaretti (n. 8)

[11] G. Deep Sharma, A. Yadav and R. Chopra, 'Artificial intelligence and effective governance: A review, critique and research agenda' (2020) 2 Sustainable Futures 100004.

earthquake, and storms. The ML model integrated in a DSS can continuously be monitored to enable better governance.

- Economy: Green economy[12] – AI will be a key enabling technology in achieving renewable energy and sustainability targets. AI can support applications such as battery storage which are helping to integrate variable power sources such as wind and solar more effectively into the electricity grids. Virtual power plants running on AI algorithms are emerging and can improve energy access and electricity trading. Solutions such as autonomous driving are transforming the mobility sector thanks to the use of AI. AI also promises major advances in energy efficiency by making our cities in particular much more responsive to the energy usage.
- Mobility: Vehicle parking and Traffic Management System[13] – Using the road surface sensors or CCTV cameras incorporated into parking spots and ML/DL algorithms allow cities to create real-time parking and traffic maps, helping drivers to save their time by avoiding waiting to find an empty space to move smoothly or be in traffic.
- Environment: Autonomous Flying Objects for Ariel View Monitoring[14] – AI-enabled and autonomous flying drones can be used to monitor the inner-city and houses or other concerning areas. The in-built cameras and DL algorithm in drones help to provide the real-time visuals of the different locations where humans cannot reach easily or quickly helping the administration and security departments to take timely actions.
- People/Living: Smart Sensing Architecture for Domestic Monitoring[15] – Smart homes play a strategic role in improving the life quality of people, enabling to monitor people at home with numerous intelligent devices. Sensors can be installed to provide continuous assistance without limiting the resident’s daily routine, giving her/him greater comfort, well-being and safety.
- People/Living: Advanced Security Camera & Surveillance System[16] – AI-enabled cameras and sensors can keep an eye on the surroundings to enhance the security level in the city’s neighborhoods. Such cameras can recognize the people and their faces or track the unusual activities done by them in restricted areas.

3.2. *Advanced Security Camera & Surveillance System*

[12] N. R. Moşteanu, A. Faccia and L. P. L. Cavaliere, ‘Digitalization and green economy-changes of business perspectives’, in *Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing* (Association for Computing Machinery 2020) 108-112.

[13] S. Saharan, N. Kumar and S. Bawa, ‘An efficient smart parking pricing system for smart city environment: A machine-learning based approach’ (2020) 106 Future Generation Computer Systems 622.

[14] O. Surinta and S. Khruahong, ‘Tracking people and objects with an autonomous unmanned aerial vehicle using face and color detection’, in 2019 *Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering* (ECTI DAMT-NCON 2019) 206-210.

[15] A. Monteriù, M. R. Prist, E. Frontoni, S. Longhi, F. Pietroni, S. Casaccia and L. Pescosolido, ‘A smart sensing architecture for domestic monitoring: methodological approach and experimental validation’ (2018) 18 Sensors 2310.

[16] R. Nawaratne, D. Alahakoon, D. De Silva and X. Yu, ‘Spatiotemporal anomaly detection using deep learning for real-time video surveillance’ (2019) 161 IEEE Transactions on Industrial Informatics 393.

As a case study, video surveillance represents one of the most active research areas in the people/living smart city action field where the AI plays a central role.[17] The main objective is to efficiently extract information from a huge amount of videos collected by surveillance cameras by automatically detecting, tracking, and recognizing objects of interest, and analyzing human behaviors.[18] Video surveillance has several applications both in public and private environments including crime prevention, homeland security, traffic control, accident prediction and detection, and monitoring patients, elderly and children at home. For instance, pre-empt future terrorist action, and providing the security of citizens at home and abroad have become top priorities in the smart city scenario for all nations worldwide. For this purpose, a huge amount of information needs to be processed, interpreted, and analyzed. In particular, this application requires monitoring indoor and outdoor scenes of airports, train stations, highways, parking lots, stores, shopping malls, and offices. The increasing availability of sensors such as RGB-D cameras, computer-based AI technologies and the growing need for safety and security in public space have attracted attention in surveillance and re-identification applications.[19]

At the same time, advanced DL methodologies have been integrated in a video-based surveillance system by research groups from academia and industry alike. In broad terms, advanced video-based surveillance system could be described as an intelligent video processing tool designed to assist security operators by providing reliable real-time alerts and to support efficient video analysis for forensic investigations.

3.3. *Benefits and challenges*

The integration of AI in smart cities has multiple benefits that can be summarized below:

- positive impact on the environmental
- optimized energy and water management and demand
- increase the accessibility of transportation system
- advance security and safety in the public.

However, there are multiple challenges that need to be solved. These challenges include infrastructure and costing, security and privacy concerns, risk of socialization and sustainability. Additionally, the design of AI algorithms as well as the overall DSS should foresee all the guidelines (see Section 1) related to the verification of reliability (ethicality) of the overall system and of all processes in the specific context.

[17] M. Paolanti and E. Frontoni, 'Multidisciplinary Pattern Recognition applications: A review' (2020) 37 Computer Science Review 100276.

[18] X. Wang, 'Intelligent multi-camera video surveillance: A review' (2013) 34 Pattern Recognition Letters 3.

[19] D. Liciotti, M. Paolanti, E. Frontoni and P. Zingaretti, 'People detection and tracking from an RGB-D camera in top-view configuration: review of challenges and applications', in *International Conference on Image Analysis and Processing* (Springer 2017) 207-218.

ELECTRIC SMART GRID

ALESSIA ARTECONI

SUMMARY: 1. Introduction. – 2. The Energy Scenario. – 3. Electric Smart Grid. – 3.1. Definition. – 3.2. Technologies. – 3.3. Demand Side Management. – 3.3.1. Demand Response. – 3.4. Blockchain and Smart Grid. – 4. Conclusions.

1. *Introduction*

This paper describes the main features of the Electric Smart Grid with reference to the present energy scenario, where it represents a key element for the process of Energy Transition. In particular, the most relevant technologies and management strategies to operate a Smart Grid are presented, describing both technical aspects and economic implications.

2. *The Energy Scenario*

The present energy scenario is characterized by an increasing penetration of renewable energy sources (RES) in the generation mix. According to the International Energy Agency, in 2018, the world total energy supply was 14 282 Mtoe, of which 13.5% was produced from renewable energy sources. Furthermore, renewable power capacity is set to expand by 50% between 2019 and 2024, led by solar photovoltaic (PV) panels. Even heat generated from renewable energy will expand by one-fifth between 2019 and 2024 and the renewable electricity used for heat is forecast to rise by more than 40%.[1]

The increasing penetration of intermittent Renewable Energy Sources introduces uncertainty in the available production capacity and require backup power and energy storage systems to ensure a reliable power supply. The example of such behavior is the famous "duck curve". The duck curve is the graphic representation of higher levels of wind and solar on the grid during the day, resulting in a high peak load in mid to late evening (see Figure 1).[2]

This behavior introduces uncertainties that challenges the traditional paradigm of the electric energy system based on a "demand following" generation, which was much easier to schedule given the predictability of the demand. On the contrary, with the increasing penetration of renewables, the uncertainty related to their energy production reflects in the energy system, both on supply and on demand side. For this reason, "the generation following" paradigm is the new target reference in the energy transition scenario. In this case the demand adapts to the generation thanks to the energy flexibility available at the user site or in the energy system (e.g. energy storage). Energy

[1] International Energy Agency, *World Energy Outlook 2019* <https://www.iea.org/reports/world-energy-outlook-2019>.

[2] D. Tait, 'The Duck Curve: what is it and what does it mean?' (29 May 2017) Energy Alabama <https://alcse.org/the-duck-curve-what-is-it-and-what-does-it-mean/>.

flexibility can compensate the uncertainty of RES production and centralized power plants can efficiently work without following the sudden changes that happen on both supply and demand side due to the variability of not predictable renewable sources.[3] In this context, smart grids play a major role.

3. *Electric Smart Grid*

3.1. *Definition*

The term Electric Smart Grid refers to a specific characterization of the electric grid, which is a network of transmission lines, substations, transformers, etc. that deliver electricity from the power plant to the final user. In particular, the adjective "Smart" is related to the introduction of sensors to monitor the grid and of the digital technology that allows for two-way communication between the utility and its customers. Indeed, the general purpose of a smart grid is to transmit energy in a controlled, smart way from generation units to consumers using a modernized infrastructure. Thanks to these features, the smart grid has the potential to revolutionize the transmission, distribution, and conservation of energy.

The benefits associated with the Smart Grid include: (i) more efficient transmission of electricity; (ii) reduced operations and management costs for utilities and consumers; (iii) reduced peak demand; (iv) increased integration of RES; (v) support to distributed generation; (vi) increased security in power supply.[4]

Furthermore, the Smart Grid helps providing consumers with timely information and control options, so that they can also act as "prosumers" in the electricity grid. The technologies at the user side that contribute to provide flexibility into the electricity grid are:

- smart meters and sensors
- energy management platforms and ICT
- electric vehicles and smart appliances
- demand side management strategies (DSM).

3.2. *Technologies*

As listed in the previous section, different technologies can be part of the Smart Grid definition and help its implementation.

Smart meters and sensors are used to collect data about electric energy taken from the grid or re-injected in case of on-site production (i.e. PV panels). They allow to monitor the users' behavior and their interaction with the grid. Thanks to smart meters, the grid managers can have the needed information about the grid status and can communicate with the final users, because they could represent a way of providing price signals or other information to manage the users' energy demand.

Information Communication Technologies (ICT) and Internet of Things (IoT) are the most important means that support the digitalization of the electric grid and allow data exchange and monitoring of the grid behavior and management. A major role for

[3] A. Arteconi, F. Caresana, G. Cesini, G. Comodi, F. Corvaro, V. D'Alessandro, G. Di Nicola, G. Latini, M. Pacetti, M. Paroncini, L. Pelagalli, F. Polonara and R. Ricci, *Energy Scenarios for the Future of Mankind in The First Outstanding 50 Years of "Università Politecnica delle Marche"* (Springer 2019).

[4] See <https://www.smartgrid.gov/the_smart_grid/smart_grid.html>.

an effective digitalization is played by the advancements in technologies together with the development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.

Electric vehicles and smart appliances (including plug-in electric and hybrid electric vehicles as well as thermal-storage air conditioning, dishwashers…) represent deferrable loads that can be integrated into the grid, acting as smart storage systems or flexibility providers. They are instruments to be used in demand side management strategies.

Demand-side management (DSM) is defined as "the planning, implementation and monitoring of those utility activities designed to influence customer use of electricity in ways that will produce desired changes in the utility's load shape, i.e., changes in the pattern and magnitude of a utility's load".[5] This concept will be further detailed in the following section.

3.3. *Demand side management strategies*

All programs intended to influence the customer's use of energy are considered demand-side management and they are aimed at increasing customer's satisfaction and simultaneously produce the desired changes in the electric utilities load in magnitude and shape.[6] In Figure 2 some examples of DSM strategies can be seen (e.g. reduce demand at peak times, reduce seasonal or annual energy consumption, shift consumption times from high cost periods to low cost periods, increase consumption during off-peak periods).

DSM can be beneficial to the power system thanks to: (i) reduced electric power peak demands; (ii) higher operational efficiency in production, transmission and distribution of electric power; (iii) lower investments for new power capacity; (iv) lower price volatility; (v) lower electricity costs and (vi) a more cost effective integration of highly intermittent renewables.[7] In the literature, three broad categories of DSM are identified: energy efficiency and conservation, onsite back up through local generation or storage and demand response. Despite its broad definition, demand side management mainly results in the implementation of four types of components: (i) energy efficient end-use devices; (ii) additional equipment, systems and controls enabling load shaping; (iii) standard control systems to turn end-use devices on/off as required; (iv) communication systems between the end-user and an external party.[8]

Given the relevance of the energy demand in buildings,[9] the management of thermostatically controllable loads in the built environment has a central role. Buildings can provide flexibility through the passive storage inherent in their envelope or by means of external active storage. On the other hand, heat pumps are efficient devices, electrically driven, which are easily coupled with building thermal mass, energy storage

[5] C. W. Gellings, *Demand-side management* (vol. 1, EPRI 1984).

[6] A. Arteconi, N. J. Hewitt and F. Polonara, 'State of the art of thermal storage for demand side management' (2012) 93 Applied Energy 371.

[7] G. Strbac, 'Demand side management: Benefits and challenges' (2008) 36 Energy Policy 4419.

[8] C. W. Gellings, *The smart grid. Enabling energy efficiency and demand response* (The Fairmont Press 2009).

[9] See European Commission website dedicated to Energy efficiency buildings <https://ec.europa.eu/energy/en/topics/energy-efficiency/buildings>.

or RES.[10] They allow to implement DSM strategies in the built environment. Through a comparative study, the different effects produced on the energy demand of electric heating systems (i.e. heat pumps) by the three different DSM categories highlighted in literature (energy efficiency, energy storage and demand response, DR) were investigated (Figure 3).[11] The main conclusions that could be drawn are:

- Energy efficiency actions can produce mainly peak shaving and energy conservation. When such action is represented by a variable capacity heat pump, the load is always present but with lower values (50% or even less).
- Energy storage systems allow load shifting. The amount of energy that can be shifted depends on the storage size and, unless in presence of external constraints, the time to which the load is moved cannot be actively controlled.
- DR operates an active load shifting to off-peak hours (valley filling) and peak shaving. In this case, energy is used in advance in comparison with the reference case. This kind of strategy tends to increase the overall energy consumption but allows a better operation of the power system avoiding high peak demand.

3.3.1. *Demand Response*

Demand response is a specific demand side management strategy. It can be distinguished in active and passive demand response. Active Demand Response (ADR) is defined as "changes in electric usage implemented directly or indirectly by end-use customers/prosumers from their current/normal consumption/injection patterns in response to certain signals".[12] In contrast, passive demand response is related to changes in the normal consumption/injection patterns without interacting with the consumers (e.g. rolling black-outs).

DR can be performed by means of price-based programs and incentive-based programs.[13] A price-based program induces a change in customers' load pattern by acting on time varying electricity rate. Different tariff structures exist:[14]

- Time-of-use (TOU): different tariffs are applied during different periods of time in a day. TOU tariffs ideally reflect the average cost of generating and delivering electric energy during the corresponding periods of time.
- Real-time pricing (RTP) or dynamic pricing: the retail price for electricity typically varies e.g. hourly on the basis of the wholesale price of electricity. Customers are generally notified in advance of the dynamic rate (on a day-ahead or hour-ahead basis).
- Critical Peak Pricing (CPP): it is a combination of the TOU and RTP tariffs. CPP is composed of TOU rates in normal times, while a peak price is used when

[10] A. Arteconi, E. Ciarrocchi, Q. Pan, F. Carducci, G. Comodi, F. Polonara and R. Wang, 'Thermal energy storage coupled with PV panels for demand side management of industrial building cooling loads' (2017) 185 Applied Energy 1984.

[11] A. Arteconi and F. Polonara, 'Assessing the Demand Side Management Potential and the Energy Flexibility of Heat Pumps in Buildings' (2018) 11 Energies 1846.

[12] X. He, L. Hancher, I. Azevedo et al., 'Shift, not drift: towards active demand response and beyond' (2013) The Florence School of Regulation <https://cadmus.eui.eu/handle/1814/27662>.

[13] A. Arteconi and K. Bruninx, '5.4 Energy Reliability and Management, (2018) 5 Comprehensive Energy Systems 134.

[14] B. Shen, G. Ghatikar, Z. Lei, J. Li, G. Wikler, P. Martin, 'The role of regulatory reforms, market changes, and technology development to make demand response a viable resource in meeting energy challenges' (2014) 130 Applied Energy 814.

specific critical conditions occur (e.g. when system reliability is compromised, or supply prices are very high).

An incentive-based program operates load reduction by means of monetary incentives (e.g. a discounted, but fixed electricity tariff or an annual payment to the consumer) to the customers. Possible incentive-based programs are:

- Direct load control: the utility remotely controls customers' electrical equipment (e.g. air conditioner, water heater) and, on short notice, it can switch them on or off on the basis of its needs.
- Interruptible/curtailable service: customers have a reduced rate if they agree to lower their demand to a certain level (curtailable rate) or even to zero (interruptible rate) during system contingencies. Typically, this program is addressed to industrial or commercial customers.
- Demand Bidding/Buyback Program: customers submit voluntarily load reduction bids to lower their load when the utility communicates the possibility to take part to a DR action, generally on a day-ahead basis.
- Emergency DR Programs: customers receive incentives to reduce their loads during emergency events.
- Economic DR Programs: customers are invited to reduce their load when the electricity price rises too high in spot events.
- Ancillary Services DR Program: customers receive incentives in exchange of load curtailment and/or fast downward ramping their demand. In this case the load modification is used as operating reserve or frequency regulation service.

3.4. *Blockchain and Smart Grid*

In order to implement effective DR programs, or, more generally, to address the challenges faced by decentralized energy systems, it is paramount to have communication platforms between the utilities and the final user and secure ways of transferring information and execute economic transactions. At this regard, blockchain technology can be of great support.

Blockchains are shared and distributed data structures or ledgers that can securely store digital transactions without using a central point of authority. More importantly, blockchains allow for the automated execution of smart contracts in peer-to-peer (P2P) networks.

Blockchains could provide innovative trading platforms where prosumers and consumers can trade interchangeably their energy surplus or flexible demand on a P2P basis. Delivering price signals and information on energy costs to consumers, they could participate to demand response programs and make a smart management of their energy demand. Blockchain is then a means to support the future energy system in: billing, sales and marketing, grid management, data transfer and automation.[15]

4. *Conclusions*

[15] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D Jenkins, P. McCallum and A. Peacock, 'Blockchain technology in the energy sector: A systematic review of challenges and opportunities' (2019) 100 Renewable and Sustainable Energy Reviews 143.

This chapter describes the Electric Smart Grid, providing its definition and the most relevant technical aspects that characterize it. Particular attention is paid to the role of demand side management strategies to realize a "generation following" operation of the grid, highlighting the role of energy flexibility as important enabler of the smart grid potential. The role of Blockchain is also presented as an instrument to unlock secure data and money transactions among different users and utilities. Through the review presented in this paper, the important role of the Electric Smart Grid for the energy transition is clearly identified.

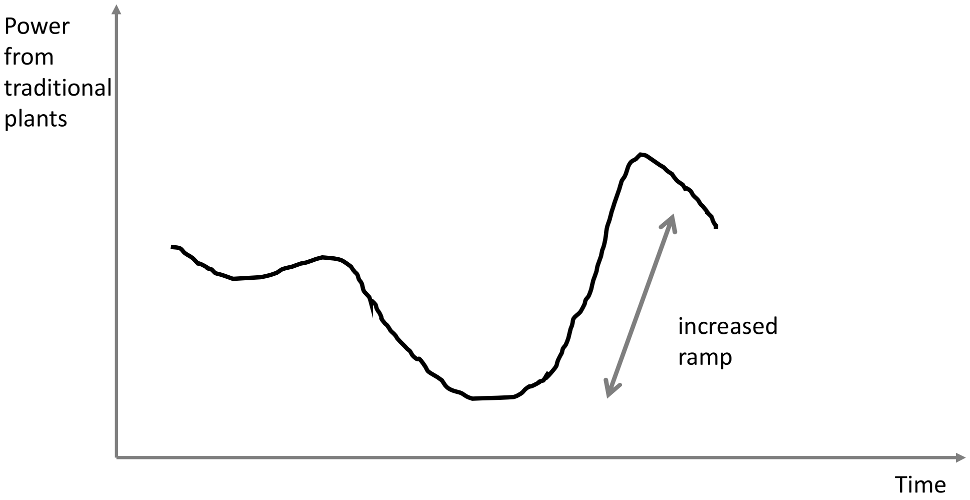


Fig. 1 – Duck curve

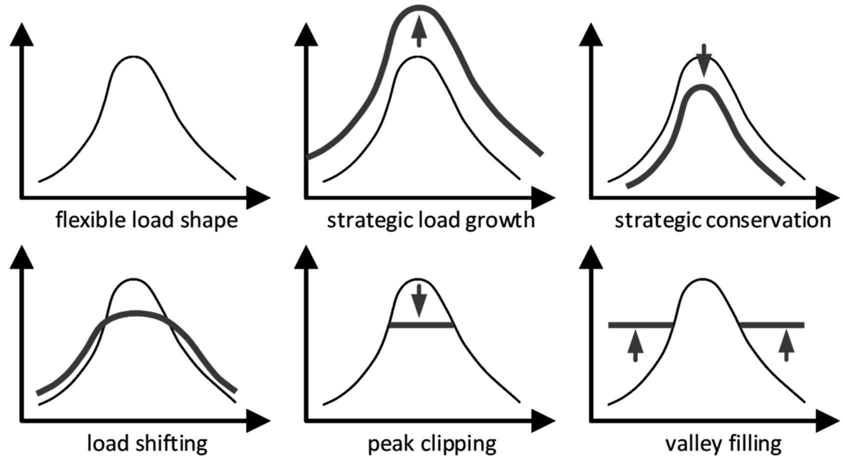


Fig. 2 – Demand Side Management strategies

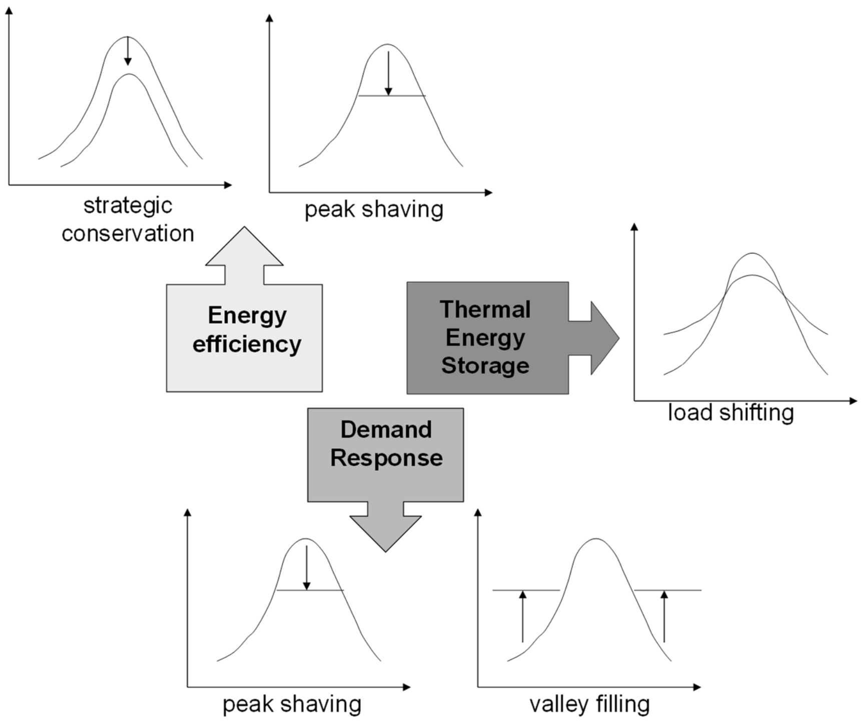


Fig.3 – Effect of different DSM strategies on the load of electric heating systems

SMART CITIES AND AIRBNB: PLATFORMS AS "REGULATORY INTERMEDIARIES" IN SHORT-TERM RENTAL MARKET?

GIACOMO MENEGUS

SUMMARY: 1. Introduction. – 2. Regulatory Intermediation in Short-term Rentals Market. – 3. Home-sharing Platforms as Regulatory Intermediaries: The Cases of France and Italy. – 4. Conclusion.

1. *Introduction*

This chapter was first conceived before the Coronavirus pandemic outburst, when the rise of home-sharing platforms like Airbnb, Homeaway, and Wimdu still seemed to be unrelenting, and cities around the world were struggling in their attempts to regulate short-term rentals. The pandemic has changed the scenario dramatically, hitting hard the whole travel industry. Airbnb was forced to lay off around 25% of its employees and it is likely to earn less than half of what it earned in 2019.[1] Travel restrictions have dried up the revenues of hosts in tourist destinations to the point that many are willing to return their houses to residents and students in the attempt to reduce their losses. It is impossible at the moment to envisage when the travel will fully return, but it will likely be different, with longer stays and a surge of rural destinations, which are perceived to be safer and secluded.[2]

It may seem therefore untimely and even counter-intuitive to investigate the effectiveness of short-term rental regulations in cities emptied by tourists.

On the contrary, this standstill period could be a unique opportunity for critical reflection on the instruments developed by lawmakers and municipal authorities to manage short-term rentals in recent years.

This chapter has this purpose. More precisely, it aims to review the increasing trend of public authorities to directly involve home-sharing platforms in the implementation, monitoring, and enforcement of relevant regulations, making them "regulatory intermediaries", as described by Christoph Busch.[3] Having regard to the technological aspects of this process, combined with the involvement of private actors in the city governance, this trend can certainly be regarded as a part of the wider rise of Smart City. The basic idea is to streamline the system of the enforcement of short-term rentals rules and to make it more efficient, taking advantage of the technological capacity of platforms and their huge data set. As will be shown, the outcomes of this "regulatory

[1] Airbnb, 'A Message from Co-Founder and CEO Brian Chesky' (5 May 2020) Airbnb <https://news.airbnb.com/a-message-from-co-founder-and-ceo-brian-chesky> accessed 20 September 2020.

[2] A. Roth, 'New Travel, New Travelers: Who Are the New Guests on Airbnb?' (24 August 2020) Airbnb <https://news.airbnb.com/new-travel-new-travelers-who-are-the-new-guests-on-airbnb/> accessed 20 September 2020.

[3] C. Busch, 'Self-Regulation and Regulatory Intermediation in the Platform Economy', in M. Cantero Gamito and H.-W. Micklitz (eds), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes* (Edward Elgar 2019) 115.

intermediation" are, however, controversial. The analysis is focused on regulatory intervention in the realm of public law, having regard to rules introduced to guarantee the right to housing, e.g. the limitation of overnight stays within one year, or to agreements reached with platforms to collect tourist taxes. Since it is impossible to cover, within this short contribution, the wide variety of different regulations and agreements adopted across Europe, the study is limited to two significant cases: the French regulation on "night limits" in large cities and the local agreements between Airbnb and Italian municipality for the collection of "*imposta di soggiorno*".

First, the notion of "regulatory intermediation" is introduced and examined with respect to its application to home-sharing platforms. Then, the issues arising from French regulation and Italian local agreements are briefly described, highlighting the strengths and weaknesses of this kind of regulatory approach. The identification of the shortcomings will eventually be brought to a conclusion, where some ways forward are proposed.

2. *Regulatory Intermediation in Short-term Rentals Market*

Traditionally, political science research on regulation and regulatory processes focused on the relationship between the regulators (or rule-makers) and recipients of the regulation (or targets). Only recently has the attention of scholarship shifted to a third subject, the so-called "regulatory intermediary". By this expression, in their seminal contribution, Abbott, Levi-Faur, and Snidal identify "any actor that acts directly or indirectly in conjunction with a regulator to affect the behavior of a target".[4] They observed that "in many circumstances, regulators lack direct access to their targets, means of influence or other capabilities necessary to regulate them, and sufficient channels for information gathering".[5] Therefore, regulator suffering from these shortcomings seeks to overcome them by involving a third party in the regulatory process: the regulatory intermediary.

This notion of regulatory intermediary is quite broad so that it encompasses a great variety of subjects ranging from "private sector actors, such as for-profit certification companies, accounting firms, or credit ratings agencies; civil society groups, such as NGO" to "governmental bodies, such as transgovernmental agency networks or international organizations".[6] According to the definition proposed, "even states can be intermediaries, for example, by promoting the compliance of other states with a mandate from the UN Security council".[7] Abbott, Lavi-Faur, and Snidal focused their analysis on intermediaries formally charged with tasks of intermediation between regulators and targets. But subsequent scientific research went on to contemplate further hypotheses, also including regulatory intermediaries with an informal character.[8] The spectrum of activities that can be carried out by intermediaries is also

[4] K. W. Abbot, D. Levi-Faur and D. Snidal, 'Theorizing Regulatory Intermediaries' (2017) 670 Annals of the American Academy of Political and Social Science 14, 19.

[5] Ibid., 15.

[6] Ibid., 18.

[7] Ibid., 15.

[8] S. Ména, L. Brès and M.-L. Salles-Djelic, 'Exploring the formal and informal roles of regulatory intermediaries in transnational multistakeholder regulation' (2019) 13 Regulation & Governance 127.

quite broad, ranging from the implementation of the rules, to the monitoring of application and enforcement of the same, up to the certification of compliance.

As noted by Christoph Busch, this broad notion of "regulatory intermediary" fits well with the case of home-sharing platforms, since "public authorities are involving platforms in their regulatory activity, drawing on their superior operational capacities and direct access to data and effective means of influencing the behavior of platform users".[9] In particular, Busch recognises the application of this intermediation process in relation to the enforcement of limits on overnight stays introduced by local regulations and state laws; and with regard to the agreements concluded with the platforms for the collection of tourist taxes.[10]

The purpose of the rules on night caps is to reduce the profit margin of the short-term rentals and thus discourage property owners from taking dwellings that were available for long-term leases and convert them to short-term Airbnb listings. For example, the city of Amsterdam introduced a 30-day cap; in Berlin, entire apartments can be rented out for a maximum of 90 days; in France, a 120-day limitation of overnight stays was recently introduced for primary residences.

The reason for the involvement of platforms, in this case, is linked to the fact that the municipalities face serious difficulties in ensuring compliance: especially in large tourist destinations, where short-term rentals can amount to thousands, it becomes impossible for municipal offices, with limited staff and resources, to verify whether hosts comply with the limit. This may entail complex investigations, cross-data analysis, and even on-site inspections since online advertisements make very little data available (not even the exact address of the accommodation). Moreover, as Oskam observed, "this labour-intensive detective work is apparently insufficient to deter hosts" from circumventing rules.[11] Even where the municipality officers make use of software that extrapolates and processes the data publicly available from the advertisements posted online, it is almost impossible to pull reliable data on the overnight stays. This software only enables the competent offices, for instance, to pinpoint accommodations that are advertised online but not registered; or to assume that there have been overnight stays not communicated to the competent offices by cross-matching non-available dates and guest reviews. However, it is impossible to calculate the exact number of overnight stays on this basis, since the relevant data are only available to the home-sharing platforms, which jealously guard the right to privacy of their users and are reluctant to hand data to public authorities.

The same goes for the collection of the tourist taxes: some hosts may not have registered their accommodations, which therefore do not appear in the databases of municipalities. Others may not correctly register their guests and stays. Others may even decide not to collect the tourist tax (in Italy, it is the duty of the host to collect the tax from tourists). Therefore, to identify any violations, it would be necessary to make use of software, to carry out cross-analysis, documentary checks, and door-to-door investigations.

The first benefit of involving platforms in the enforcement of these regulations is therefore effectiveness. As Busch stated, citing Michèle Finck, "platforms have a much

[9] Busch (n 3), 120-121.

[10] Ibid., 121-123.

[11] J. A. Oskam, *The Future of Airbnb and the 'Sharing Economy' The collaborative Consumption of our Cities* (Channel View Publications 2019), 99.

higher success rate in ensuring tax and legal compliance than public regulators, as they can, 'through a simple twisting of code', secure that platform users pay taxes and comply with time-limits".[12] A further advantage is given by the considerable simplification of administrative aspects and procedural burdens, both for platform users and public administrations. Once the limit of nights is reached, the advertisement is automatically delisted, without the need for any intervention by the host or the municipality. The tourist tax is collected via platform together with the payment of the stay.

The overall picture thus looks very promising in terms of simplification and improvement of the governance of the short-term rentals market. However, upon closer inspection, several issues emerge that are worthy of attention. First of all, transparency issues have been raised vis-à-vis the platforms since the data they process to perform their regulatory intermediation tasks are still not shared with public authorities. Airbnb sometimes consents to data transfers in aggregate form but in such a way as to prevent identification of single users or to render control by the authorities particularly complex. These aspects cast a shadow on the reliability of the regulatory intermediation of platforms since checking the enforcement correctness depends on an act of trust of the municipal administrations in the platforms. The latter, in any case, have no real interest in uncovering any evasive behaviour of their users and thus damage the reputation of the platform itself. Besides, there are elements to question the legitimacy of the contents of the tourist tax agreements. And doubts emerge even about the very effectiveness of the regulatory intermediation mechanism because many aspects still remain beyond the control of the platforms.

3. *Home-sharing Platforms as Regulatory Intermediaries: The Cases of France and Italy*

Issues of transparency, legitimacy, and effectiveness can be further explored through the analysis of two specific cases: the French regulation on overnight stays and the agreements between Airbnb and Italian municipalities for the collection of tourist tax.

In recent years, France has been among the most active European Member States in regulating tourist rentals, adopting three important laws, which followed one another over a few years and reformed the legal framework for tourist rentals.[13]

The French law distinguishes between primary and secondary residences.

To rent out their primary residence, owners do not need any authorisation, registration being necessary (and sufficient) in large cities. However, it is not possible to rent out the primary house for more than 120 days a year. If the owners intend to exceed this limit, they are required to file a change of use of the dwelling, which will thus be considered a secondary residence.

For secondary residences (i.e. dwellings where the owners live less than four months a year) it is necessary to distinguish between the areas in which they are located; in fact, where the house is located in areas with shortages of rental housing (cities with over

[12] Busch (n 3), 122 citing M. Finck, 'Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy' (2017) Law Society and Economy Working Papers 1, 21 <https://ssrn.com/abstract=2990043> accessed 20 September 2020.

[13] Loi n° 2014-366 du 24 mars 2014 pour l'accès au logement et un urbanisme rénové (Loi ALUR) (2014); Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (2016); Loi n° 2018-1021 du 23 novembre 2018 portant évolution du logement, de l'aménagement et du numérique (Loi ÉLAN) (2018).

200,000 inhabitants and some departments close to Paris), the owner must request authorisation for the change of use. In some areas, where the shortage of rental housing is particularly severe (e.g. in Paris), in order not to further reduce the property stock on the rental market, such an authorisation is made conditional by the municipal rules upon an offset requirement in the form of the concurrent conversion of non-residential premises into housing.[14] Single room rentals in a primary residence are, however, not subject to any registration or authorisation scheme.

In order to monitor compliance with this regulatory framework, registration duties are prescribed for hosts along with the duty for platforms to remove advertisements without registration numbers displayed and to block accommodations that have reached the abovementioned 120-day cap.

In June 2018, on the basis of an agreement with the French government, Airbnb and other home-sharing platforms committed themselves to introduce an automatic tool to ensure that primary residences cannot be booked for more than 120 days per year.[15]

The actual performance of this enforcing mechanism is highly controversial. Starting from 1 January 2019, platforms are required to transmit a series of data to the municipalities for each calendar year, including the address of the accommodation and the number of overnight stays.[16] Airbnb first published data in late December 2019 that shows only about 4100 hosts have exceeded the 120-day cap, all of them allegedly in accordance to exemptions provided by law.[17] The platform presented the results as a great success, claiming that the automatic block reduced the number of residences rented out for more than 120 days by more than 40%.[18] The City of Paris contested the data provided by Airbnb, arguing (on the basis of data processed by the site InsideAirbnb) that the platform does not properly communicate the data and does not fully apply the 120-day cap.

There are serious elements to question platform enforcement activity.

First of all, the platform does not verify if the information regarding the status of the accommodation is correct. Hosts may enter false or incomplete information and Airbnb is not able to check it since it would entail documentary and door-to-door inspections. Exceptions provided by law offer simple workarounds to hosts. As data analysis and simple Internet research have shown, it is easy for hosts to recategorise an entire house as a single room, circumventing the overnight stays limits.[19] But the aspect that challenges the effectiveness of the entire control mechanism is that the automatic cap

[14] Various aspects of this regulatory framework have been recently reviewed by the Court of Justice of the EU found to comply with EU law: see Court of Justice of the EU (Grand Chamber), Joined Cases C-724/18 and C-727/18, *Cali Apartments SCI and HX v Procureur général près la cour d'appel de Paris and Ville de Paris*, judgment of 22 September 2020.

[15] Airbnb, 'World premiere: Airbnb, Abritel/HomeAway, Le Bon Coin, TripAdvisor commit to sustainable tourism together with the French Government' (16 June 2018) Airbnb <https://news.airbnb.com/world-premiere-airbnb-abritel-homeaway-le-bon-coin-tripadvisor-commit-to-sustainable-tourism-together-with-the-french-government/> accessed 20 September 2020.

[16] Décret n° 2019-1104 du 30 octobre 2019 pris en application des articles L. 324-1-1 et L. 324-2-1 du code du tourisme et relatif aux demandes d'information pouvant être adressées par les communes aux intermédiaires de location de meublés de tourisme.

[17] E. Donada, 'Location à Paris : les chiffres publiés par Airbnb sont-ils sous-estimés ?' (24 December 2019) Libération <https://www.liberation.fr/checknews/2019/12/24/location-a-paris-les-chiffres-publies-par-airbnb-sont-ils-sous-estimes_1770765>.

[18] Ibid.

[19] Ibid.; see also Oskam (n 11) 97.

is admittedly applied by Airbnb only to listings that have a registration number.[20] This means that 80% of Parisian listings are outside the control of the platform since only 20% (as both the town hall and Airbnb confirmed) have applied for and obtained a registration number.[21] The reluctance to share additional data (such as the listings' URL) to facilitate the municipality's checks does not allow for a clear picture of the number of violations. But this certainly does not speak in favour of the platform, which in doing so feeds requests for greater transparency.

Issues that are partly similar and partly different arise with respect to the various agreements reached between Airbnb and numerous Italian cities for the collection of the tourist tax.[22] On the basis of such agreements, the guest is basically required to pay the tax at the time of stay via payment platform, which then remits to city authorities the entire amount of the taxes collected on a regular basis (so-called collect and remit mechanism). In this case, there is no legal obligation for the platforms to collect the tax. These are commitments undertaken voluntarily which benefit intermediaries, users, and local administrations. The latter have a "guaranteed revenue" and are relieved from controls and administrative tasks. The hosts do not have to ask the guest for the tax, fulfil registration duties, and pay it back to the city. The guests pay it all in one lump sum. The platform obtains an *ad hoc* simplification of the tourist tax for its users and also enjoys a certain return in terms of reputation, being able to present itself as "willing to cooperate" with the local administrations.

The counterpart for this tourist tax collection service consists, as seen, in the *ad hoc* simplification of the amount and the calculation of the same tax only for Airbnb. However, the terms of the simplification are subject to negotiation between the parties and Airbnb is likely to have a greater contractual weight.[23]

In some cases, the Airbnb rate is fixed, in others, it is calculated as a percentage (for example 6%) on the amount for the stay, but is often different from that applied to the other apartments rented out for tourists. This raises issues of legitimacy: given that the taxpayers of the tourist tax are tourists, how can the different treatment between guests staying in a flat rented on Airbnb and those who instead stay overnight in another booked on a different platform be justified? Having regard to the fact that the same host can advertise her or his home on different home-sharing platforms, how can it be that tourists who stay at different times in the same apartment, but book through different portals, pay different taxes? Another controversial aspect is related to the data shared with the municipalities: Airbnb merely transfers the total number of nights and taxes recovered. These elements are far from useful for understanding if Airbnb did its job. Once again, the platform is willing to transfer only aggregate and statistical data.

[20] D. Lacaze, 'Ces villes où Airbnb met en place la limitation automatique à 120 jours par an' (2 January 2019) BFM Immo <https://www.lavieimmo.com/immobilier-paris-36806/ces-villes-ou-airbnb-met-en-place-la-limitation-automatique-a-120-jours-par-an-44374.html>.

[21] Ibid.

[22] For an overview of the current agreements in Italy see Airbnb, 'Occupancy tax collection and remittance by Airbnb in Italy' <https://www.airbnb.co.uk/help/article/2287/occupancy-tax-collection-and-remittance-by-airbnb-in-italy?_set_bev_on_new_domain=1600418677_YGujf9TlWpCFNL%2F0>. For an example of such agreements (with English translation) see: 'Agreement concerning the implementation, collection and remittance of Tourist Tax' between the City of La Spezia and Airbnb Ireland <http://www.speziarisorse.it/servizi-online/imposta-di-soggiorno/>.

[23] Oskam (n 11), 94.

The agreements usually provide for mechanisms to allow the municipality offices, upon request and in specific cases, to control the correctness of the collection, which however appear to be surrounded by cautions and reservations in sharing more detailed data.

4. *Conclusion*

This chapter has examined the concept of regulatory intermediation in its applications to home-sharing platforms. In the context of the wider rise of the Smart City, the involvement of platforms for enforcing short-term rental regulations can be regarded as a way to simplify and improve controls and effectiveness of the rules. The analysis of two case studies – the French 120-day cap and the Italian local agreements for the tourist tax collection – shed some light on the shortcomings of such an approach. The controls are apparently not as effective as one might have imagined. Users have workarounds and the platform does not seem able (or willing) to identify them. The existing information asymmetry, increased by platforms' reluctance to share data, places public authorities in the position of not being able to assess whether platforms comply with their obligations, and implement the rules correctly. Their superior operational capabilities and the greater bargaining power also seem to trigger processes of capture of the regulator by the intermediary. This is the case of the agreements for the collection of tourist taxes.

The only way forward is to overcome the information asymmetries. A possible solution is to introduce new disclosure obligations for the platforms. Examples are offered by France in 2019[24] and by the City of Vienna in 2016.[25] However, this kind of regulatory intervention has the drawback of adding further administrative burdens. The most promising solution, as highlighted by different authors, would be instead to introduce APIs tailored to government auditing purposes.[26] A significant example in this sense is offered by the API adopted by the city of San Francisco.[27] To avoid excessive fragmentation and complication of the process, a single regulatory initiative at the European Union level would be more appropriate. Encouraging steps in this regard can be seen in the agreement concluded by the Commission with Airbnb, Booking.com, Expedia Group, and Tripadvisor on statistical data sharing.[28] But the road is still long.

[24] Décret n° 2019-1104 du 30 octobre 2019 (n 16).

[25] Busch (n 3), 122.

[26] Finck (n 12), 23, Busch (n 3), 123.

[27] Busch (n 3), 123.

[28] European Commission, 'Commission reaches agreement with collaborative economy platforms to publish key data on tourism accommodation', Press Release, 5 March 2020 <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_194> accessed 20 September 2020.

Technological Innovation and Artificial Intelligence Applied to Intermodal Transport: The Case Study of the Port of Ancona

MATTEO PAROLI

SUMMARY: 1. Introduction. – 2. The Port of Ancona and its role in the motorways of the seas. – 3. The challenge to increase the port areas in an urban port. – 3.1. The TinS Global Project. – 3.1.1. The customs procedure and the infrastructural constraints – 3.1.2. The need for an innovative approach. – 3.1.3. How to implement Artificial Intelligence in ports? – 3.2. The TinS implementation. – 3.2.1. The TinS project main phases. – 3.2.2. Benefits and awards of the TinS project.

1. *Introduction*

One of the characteristics of the Italian port system concerns the proximity of the ports to the urban area, unlike many other ports in Northern Europe, that moved the terminals for commercial traffic away from the city area, with the exception of passengers facilities. This peculiarity makes it necessary to pay particular attention to the adoption of measures to mitigate the pollution deriving from port activities with respect to the residential and city functions of the areas adjacent to the ports. This is particularly relevant for the Port of Ancona, where the urban conformation and the development of the port involve that ferries are moored in docks close to the historic center. This contribution will present the case of the application of Artificial Intelligence technologies to solve the issue of the lack of spaces and port congestion in one of the main nodes of the Motorways of the Seas of the Eastern Mediterranean.

2. *The Port of Ancona and its role in the motorways of the seas*

The Port of Ancona is one of the main European terminals for the Motorways of the seas, i.e. the ferry lines that connect on regular basis Ancona with Igoumenitsa and Patras in Greece, Split and Zadar in Croatia and Durres in Albania. More than 140.000 loading units are embarked and disembarked every year, for an annual throughput of 4,7 million tons of cargo and more than 1 million passengers[1]. Although the COVID-19 pandemic is having a severe impact on passengers' traffic, the cargo volume has experienced an important decrease (-16% up to August 2020), but nonetheless the lines remained regular.

The Adriatic-Ionian Sea basin is defined by the EUSAIR Strategy[2] as "a natural waterway penetrating deep into the EU. […] There is potential for improved land-sea connectivity and intermodal transportation, increasing the competitiveness of hinterland economies". Therefore, the macro-regional strategy insists on the

[1] Statistical data on freight and passenger traffic of the port of Ancona in the last 3 years: freight traffic (in Mil of tonnes): 11, 038 in 2017, 10,819 in 2018 and 10,767 in 2019. Passenger traffic (in mil of passengers): 1,091 in 2017, 1,515 in 2018 and 1,189 in 2019

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions concerning the European Union Strategy for the Adriatic and Ionian Region, COM(2014) 357 final, 17 June 2014.

improvement of the connections between ports and hinterland areas, to support the regional economies, and increase the sustainability of the freight flows.

The traffic analysis implemented by the MoS coordinator in the framework of the MoS Detailed Implementation Plan 2020 clearly shows the main container and ferry traffic flows on the North-South and East-West directions across the Adriatic and Ionian seas, linking the hinterland regions of South Eastern Europe with Italy and the continental Europe (Figure 1).

3. *The challenge to increase the port areas in an urban port*

The ferry traffic is operated in the historical port of Ancona, close to the town centre. The lack of space behind the port brought to the decision to move the check in terminal and the parking areas away from the quays, in order to improve the organization of the traffic flows and comply with the security standards for maritime traffic.

However, there was the need for dedicated parking inside the customs area in the port to implement the customs formalities before boarding or after disembarking. As a first solution, trucks were parked on the *Molo Rizzo* pier, an infrastructure for cargo traffic that was dismissed in 2014 in the Old Port area. But its position proved to be inefficient because of the lack of a sufficient number of parking lots, distance from the customs offices and the ferry terminal for check-in operations, lack of the basic services for truck drivers that were also far from the town centre. Last but not least, the area surrounding the *Molo Rizzo* pier hosts some of the most impressive remnants of the Roman port, including the Arch of Trajan, dating back to the second Century A.D. (Figures 2-3)[3].

In order to find an innovative approach in the management of the MoS traffic, the Central Adriatic Ports Authority (ADSPMAC) launched a feasibility study to assess technological solutions to solve the issue related to customs formalities.

3.1. *The TinS Global Project*

3.1.1. *The customs procedure and the infrastructural constraints*

With regard to landing operations, all trucks arriving in the port are subject to the controls of the customs authorities, the Customs Agency (*Agenzia delle Dogane*) and the Customs police named *Guardia di Finanza*. The customs authorities, according to the Union Customs Code are required to carry out the checks necessary to guarantee the supervision of international trade for goods entering and leaving the territory of the European Union (EU) [4].

[3] According to the "Cultural Heritage and Landscape Code" (Legislative Decree 22 January 2004, No. 42), the administrative responsibilities for the conservation and management of cultural heritage lies with the Ministry of Cultural heritage and activities; however, the same code states, at the art. 30, that each public body is in charge of ensuring the maintenance and conservation of cultural heritage under its territorial competence.

[4] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code. Art. 3: "Customs authorities shall be primarily responsible for the supervision of the Union's international trade, thereby contributing to fair and open trade, to the implementation of the external aspects of the internal market, of the common trade policy and of the other common Union policies having a bearing on trade, and to overall supply chain security. [...]". Art 46: "The customs authorities may carry out any customs controls they deem necessary [...]".

These controls take place in specific places designated by the customs authorities, where the goods must be brought as soon as they arrive in the European territory and from which they can leave only after having completed the relative procedures.

Until 2018 customs formalities and controls were implemented in the Port of Ancona in an area close to the Old Port with Roman and other historic remains, as mentioned above.

The need to optimize the spaces and the ferry traffic has prompted Central Adriatic Ports Authority (ADSPMAC) to identify a parking area outside the port customs spaces, called "*Scalo Marotti*", where to transfer the trucks unloaded from the ships and undergo the customs formalities and controls. The *Scalo Marotti* is a former railway yard, and it was already available for port operations. In August 2018 it became property of ADSPMAC (31.000 sqm). The Customs Agency included the *Scalo Marotti* as customs storage facility[5].

To improve the quality of service and face the traffic growth, ADSPMAC and the Customs Agency decided to launch an innovative project aimed at shifting the customs parking outside the ferry port customs gate. The project was named *TinS – Trasferimento in sicurezza* (Secure transfer). The TinS feasibility study confirmed the "*Scalo Marotti*" as the best solution to set up the new customs parking (Figure 3). The study proposed the proper juridical framework, the infrastructural needs and a first sample of technological solutions to ensure the tracing and tracking of the vehicles along the road between the *Scalo Marotti* and the customs gate. Following the positive assessment of the feasibility study, the port authority, the Customs Agency and the *Guardia di Finanza* decided to start a testing phase "on the field" to assess potential negative impacts on the port traffic flows and control systems. The testing phase demonstrated the feasibility of the project. The main results of testing in the months of June and July were:

- No impact/very small impact on ferry traffic timetable, notwithstanding the peak season traffic flows (touristic flows on ferries travelling together with commercial vehicles).
- Road traffic was never blocked notwithstanding the adding of the traffic related to the *Scalo Marotti* along the road linking the *Scalo Marotti* to the customs gate and vice versa.
- The feasibility of the trucks and vehicle monitoring and the capacity to separate the customs traffic flows from the non-customs traffic flows.
- A relevant result of the testing was an estimated reduction of 11.000 km of driving of heavy good vehicles (HGV) in 2 months of testing inside the port facilities close to Ancona town centre.
- The need for an automated control of the traffic flows to reduce the Custom police and the traffic assistance staff along the road, with a positive impact on increasing the control capacity, reducing costs and the risks for the human resources deployed along the road.

3.1.2. *The need for an innovative approach*

The challenge was how to allow trucks to reach the *Scalo Marotti* area, passing along an ordinary urban road, not subject to customs controls.

[5] This operation was officially authorized by the Customs Agency with the Procedure 16242/RU.

This would have entailed a series of risks, including, for example, the deviation from the route or the escape of the truck, without prior control; an alteration of the load; the removal of goods and other possible illegal situations with respect to transport.

As first alternative, the TinS feasibility study designed an organization based on the sealing of each truck upon disembarkation from the ship, applying a GPS georeferencing sensor for control[6]. Although the costs were bearable in economic terms, they certainly would not have been in terms of temporal impact on the individual embarkation and disembarkation operations. In fact, the need to seal the trucks upon disembarkation and to remove the seals and GPS sensors when parking in the area subject to customs control, would have compromised the disembarkation of the vehicles from the ferries. Furthermore, this type of control would have required the presence of additional personnel to carry out this operation (2 people at disembarkation, 2 at the final parking destination), making the timing of the operations unacceptable, considering the significant slowdown caused by an average of about 70 trucks stopped for 5 minutes each, for each ferry[7].

As an alternative to this first hypothesis, which is not feasible, ADSPMAC has chosen to make use of the technology developed by an Italian company, Hyperion Software S.R.L.,[8] that developed a software of Artificial Intelligence created with the aim of monitoring automatically, without the intervention of operators, sensitive perimeters and paths. A solid technology, already in use both in Italy and abroad for civil and military purposes, that proved its effectiveness and maturity in the real testing that were implemented during the comparative process opened according to the rules for public tenders: although several operators declared in principle the availability of alternative software of Artificial Intelligence, no one was able to carry out tests on the field, except the A3iu software developed by Hyperion S.R.L.[9]

After the market consultation, in January 2019, ADSPMAC started the acquisition process and the installation of the Artificial Intelligence system in the framework of the TinS Global Project.

3.1.3. *How to implement Artificial Intelligence in ports?*

The A3iu Artificial Intelligence software works on the data collected by high-definition IP cameras and it is able to transform the image of vehicles in objects to be monitored. The software therefore can identify people, and vehicles, both light and heavy, so it is able to discriminate a truck from a car. Furthermore, it records images and recognizes license plates, associating them with each single vehicle. This made it possible to avoid any type of hardware tool to be applied on trucks, both a seal and a GPS georeferencing sensor, because the vehicle, without any type of compulsory stop at the time of disembarkation, can exit the port gate being controlled by customs authorities and traced, continuously, in the 800 m of urban path that separates the port

[6] The GPS (Global Positioning System) is a satellite-based radionavigation system that provides geolocation and time information to a GPS receiver anywhere on or near the Earth. The application of a GPS sensor in each truck disembarking at the port would allow the tracking and tracing of any truck movement inside the port area.

[7] The average disembarking time for a vehicle at the port of Ancona, from the exit ramp of the ship to the terminal gate of the port, is round one minute.

[8] See <http://www.hyperionsoftware.eu>.

[9] See <http://www.hyperionsrl.eu>.

customs areas with the customs parking outside. Another relevant feature is the capacity of the Artificial Intelligence system to recognize and follow the vehicle, tracing it automatically without the need for interaction or intervention by a human operator. In case of unconformities, the software alerts the customs officer or the financial police officer in charge of the controls, who can immediately assess the situation and take the proper decisions.

The technology backbone consists of the Artificial Intelligence based video analysis, which allows the merging of images, coming from multiple concurrent sources (cameras and plate recognition systems), sharing the same space. Non-camera based sensors can also be correlated to the merged video streams, to propose a virtual 3D representation of the space where all the entities are identified, classified and geo-referenced. A neural network-based engine continuously elaborates signals and events, which are part of the virtual 3D model, for the generation of alarms according to rules created by users. It merges, analyses and evaluates information coming from various sensors to react to events and minimizes false alarms, as A3iu is able to differentiate between relevant and irrelevant information. Concerning privacy, A3iu enables the anonymity of the monitored targets visualizing avatars in the 3D Virtual User Interface. The expected results are the following:

- Increased automation: video as well as other type of content is georeferenced in a 3D setting and rendered to the user in a virtual reality interface eliminating the need of monitors and dedicated personnel.
- Increased security and reaction: the Artificial Intelligence system on which it is based performs a deep analysis of the data received reducing the number of false alarms to irrelevant levels, but targeting all the suspicious behaviours, making available tools to countermeasures in case of dangers and alerts. The system also makes available relevant data for investigations and training.
- Increased management capacity: port operators as assistance staff and *Guardia di Finanza* can control and manage in real time the ferry related traffic flows in- and outbound the port. The capacity is not limited to the vehicles implementing customs formalities; it is rather extended to all the vehicles and people passing through the road.
- Replicability: testing and validation of a best practice to optimize vehicle traffic monitoring, tracking, tracing and control with specific reference to international ferry traffic servicing also third countries.

3.2. *The TinS implementation*

The project is managed by ADSPMAC, in close cooperation with the local offices of the Customs Agency and the *Guardia di Finanza*. The port authority is in charge for the infrastructural works and the setup of the ICT system. The Customs Agency is in charge of the assessment of the consistency of the procedure with the Union Customs Code and to define the requirements related to the new facilities to perform customs formalities and inspections. The *Guardia di Finanza* is in charge of assessing the innovative procedure on the side of customs controls and it is the main beneficiary from the ICT system deployment.

The project will include the economic, juridical, operational and environmental studies aimed at providing ADSPMAC and the Customs Agency the information on the overall costs and benefits of the pilot project[10], the best practices to reply in other ports or customs facilities and the added value for a port authority deriving from the deployment of an AI technology in terms of data management, port infrastructure management, traffic flow control, safety and security. An in-depth analysis will also be implemented to assess the positive impact in terms of reduced pollution coming from the reorganization of the customs related services for the ferry traffic of the Port of Ancona[11].

The main indicators to assess the pilot action are:

- Impact on human resources needed for the management of the traffic flows
- Reduction of HGV path in the port premises close to the town centre compared with the previous solution
- Queueing time along the virtual corridor
- Improved availability of traffic statistical data related to ferries
- Number of anomalous behaviors detected by the system
- Number of days for the learning of the system and reduction of the false alarms
- Number and type of ICT equipment coordinated by the Artificial Intelligence.

3.2.1. *The TinS project main phases*

The TinS project is articulated in the following activities:

- Activity 1.1: The activity consists in the acquisition of the A3iu licence from the owner Hyperion S.R.L.
- Activity 1.2: Acquisition of the ICT/digital equipment to allow the implementation of the project.
- Activity 1.3: Implementation, testing and management of the software for the information exchange between the A3iu Artificial Intelligence, the Customs Agency software and the freight forwarders and maritime agents databases. The objective is to provide to the Artificial Intelligence the proper instructions about the vehicles embarking and disembarking in the port. Concerning customs formalities, the timely sharing of the cargo manifests will allow the software to identify the vehicles that shall perform customs formalities.

[10] According to the Horizon 2020 EU Programme, a pilot project is intended as a project aimed at validating the technical and economic viability of a new or improved technology, in an operational (or near to operational) environment, whether industrial or otherwise, involving where appropriate a larger scale prototype or demonstrator.

[11] Central Adriatic Ports Authority, in cooperation with the Municipality of Ancona and the Marche Region developed the "PIA" project ("Progetto Inquinamento Ancona", Ancona Pollution Project), aimed at improving knowledge on the exposure of the population to allergenic pollens and their potential interaction with pollutants atmospheric agents such as fine dust (PM 10 and PM 2.5). The project consists also in the realization of actions aimed at increasing the awareness of institutions and citizens on the issue of air quality through integrated information, communication and education activities to encourage the adoption of correct lifestyles, especially for the most sensitive population groups. The project focussed on four issues of strategic interest: Health; Environmental monitoring of inorganic pollutants with particular regard to PM 2.5; Role of urban greenery as a pollutant of a biological nature or as a factor for mitigating damage from pollution; Communication strategy. In the context of "PIA" project, Central Adriatic Ports Authority focussed on the analysis of the emission framework relating to the port of Ancona, especially as regards maritime traffic and road traffic, in order to assess the impact on the air quality at the local scale and in the urban basin, both at present and in perspective, in correspondence with future transport, logistics and intermodality scenarios for the Adriatic-Ionian Macro-region.

Currently all the activities are under implementation and the first test of the integrated solution is planned by the end of 2020.

3.2.2. *Benefits and awards of the TinS project*

Considering the innovative character and the scope of application to intermodal transport[12], the TinS project has obtained significant awards, such as the assignment of the "SMAU 2019 innovation award", as well as the EU co-financing equivalent to 50% of the expected technological investments (Project Smart-C, CEF Program, Innovation 2018 Call - Total budget € 1,083,561.00, of which EU contribution € 541,780.00).

This mechanism generates significant cost and time savings, a fundamental aspect in the logistics of goods transport, even more than the initial cost of the service.

Finally, the positive environmental value of this project must be absolutely underlined, which allowed ADSPMAC to avoid the travel by heavy vehicles of about 60,000 km of total traffic per year, thanks to the optimization of the route to comply with the controls by the Customs Agency and the *Guardia di Finanza* with a significant benefit in terms of reducing pollutants on the neighboring city spaces (an assessment on the reduced environmental impact is presented in Table 1). This generates advantages, from various points of view and for different stakeholders.

First of all, it is important to point out that, from the entry into force of the automatic control system shown, there is a significant benefit for the environment, which is highlighted by the important reduction in polluting emissions shown in the table above, which generates a direct benefit for the city of Ancona itself, overlooking the port area. The Italian ports are all, with very rare exceptions, as already mentioned, contiguous to the city environment, therefore the optimization of the route of heavy vehicles in an area so delicate from an architectural, cultural and landscape point of view, like that of the Port of Ancona is an undoubted advantage also in terms of the impact that these vehicles could have on the city, not far from the port.

Furthermore, it has an advantage in terms of efficiency in carrying out the entire customs procedure, creating a widespread benefit for all elements of the logistics chain, as well as for the operators themselves involved (truck drivers, shippers, transporters), as they can achieve transfers. inside the port thanks to the knowledge of the destination during the unloading phase, which foresees a straight path of 800 m, instead of about 1,5 km, which would have involved unnecessary journeys.

Finally, ADSPMAC project interprets and adapts the provisions of EU law in a modern key, in compliance with the provisions of the Union Customs Code mentioned at the beginning. In particular, Art. 134 "Customs Vigilance" provides that goods introduced into the customs territory of the EU are subject to customs supervision, can undergo customs controls and cannot be removed without customs authorization. Furthermore, the following Art. 135 "Transport to the appropriate place" provides that goods brought into the customs territory of the EU are transported without delay, following the route indicated by the customs authorities, to the place designated by those authorities.

[12] Intermodal Transport refers to the use of different modes (or means) of transport on the same journey. The optimal combination of different modes of transport ensures efficiency, cost and time reduction of transport operation and contributes to reduce the environmental impact of heavy traffic flows.

Today, thanks to the application of the above technological innovation and software to intermodal transport, the place in charge of carrying out these checks is represented by *Scalo Marotti*, thus allowing the Port of Ancona to ensure timely and punctual checks on goods and vehicles. in transit, combining safety, sustainability and efficiency both for loading / unloading operations, and in terms of reducing pollutants, which have always been attributable to this type of traffic.

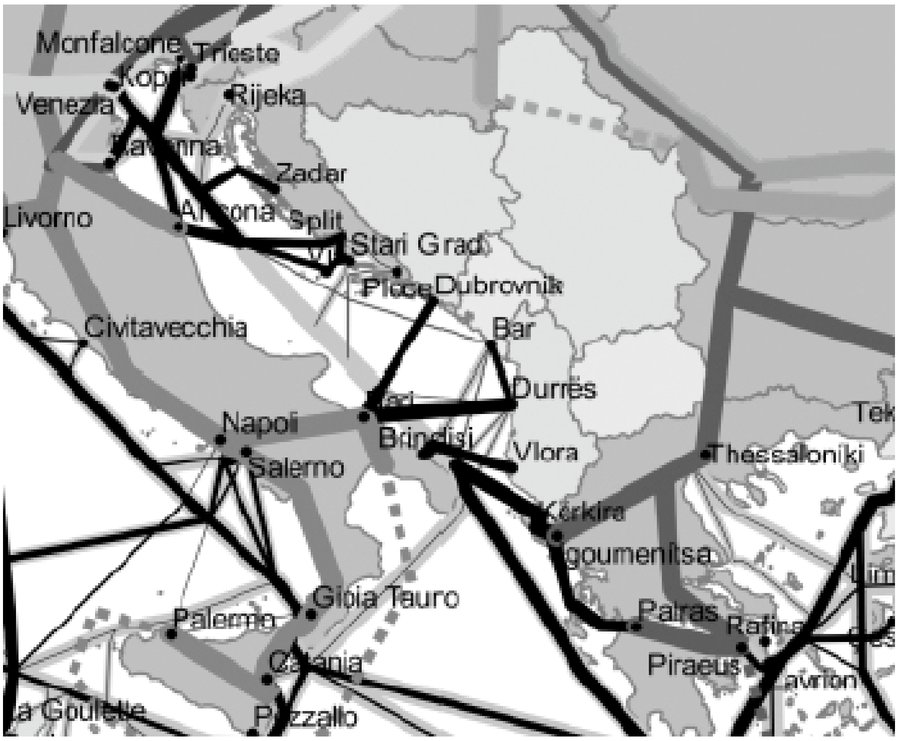


Fig. 1: MOS DIP 2020. Regular container and RORO ferries in the East MED (Elaboration: Central Adriatic Ports Authority)

Pollutant	Category	Fuel	Segment	Euro Standard	CO 2017 g/km U	KM saved	Total emission saved (kg)
CO	Heavy Duty Trucks	Diesel	Articulated 14 - 20 t	Euro III	2.1856	60,000	131.136
CO2	Heavy Duty Trucks	Diesel	Articulated 14 - 20 t	Euro III	853.8276	60,000	51,229.656
NMVOC	Heavy Duty Trucks	Diesel	Articulated 14 - 20 t	Euro III	0.3875	60,000	23.250
NOX	Heavy Duty Trucks	Diesel	Articulated 14 - 20 t	Euro III	7.6112	60,000	456.672
PM 10	Heavy Duty Trucks	Diesel	Articulated 14 - 20 t	Euro III	0.3158	60,000	18.948

Table 1: Emissions saved as result of the TinS project

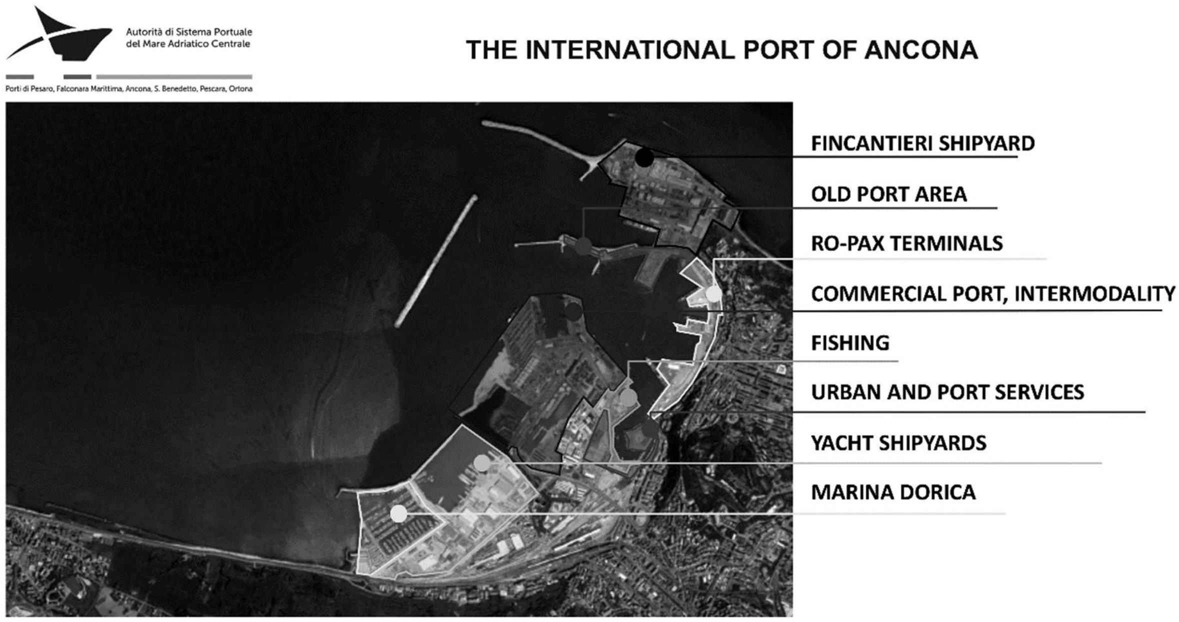

Autorità di Sistema Portuale
del Mare Adriatico Centrale
Porti di Pesaro, Falconara Marittima, Ancona, S. Benedetto, Pescara, Ortona
THE INTERNATIONAL PORT OF ANCONA
FINCANTIERI SHIPYARD
OLD PORT AREA
RO-PAX TERMINALS
COMMERCIAL PORT, INTERMODALITY
FISHING
URBAN AND PORT SERVICES
YACHT SHIPYARDS
MARINA DORICA

Fig. 2: The international port of Ancona. Evidence of the ferry terminal and of the old port area

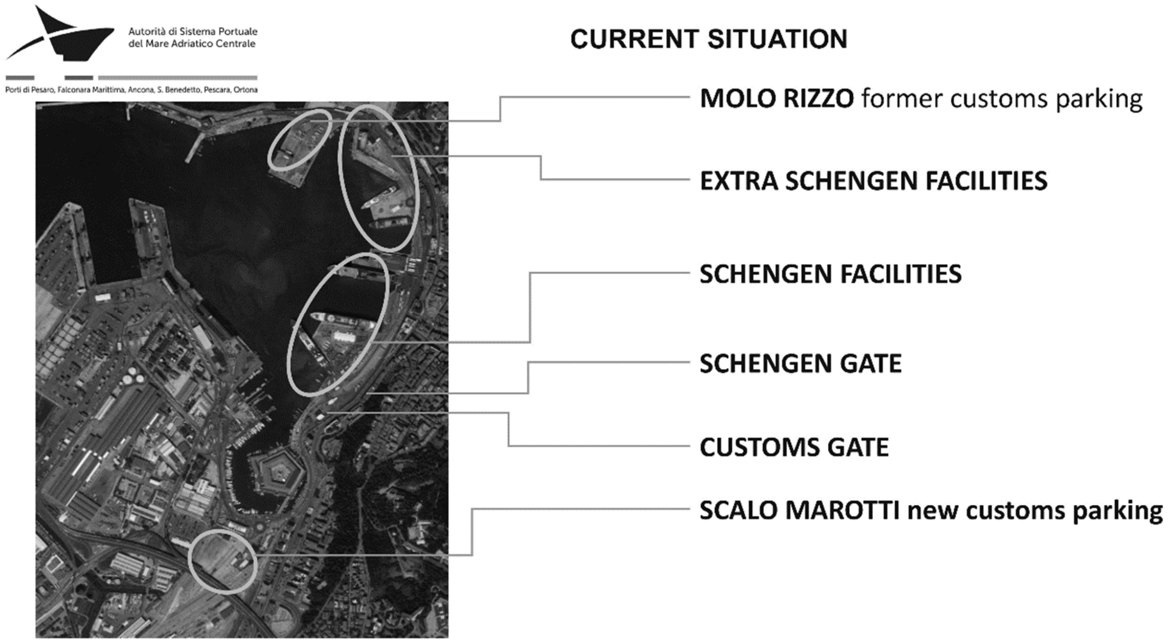

Autorità di Sistema Portuale
del Mare Adriatico Centrale
Porti di Pesaro, Falconara Marittima, Ancona, S. Benedetto, Pescara, Ortona
CURRENT SITUATION
MOLO RIZZO former customs parking
EXTRA SCHENGEN FACILITIES
SCHENGEN FACILITIES
SCHENGEN GATE
CUSTOMS GATE
SCALO MAROTTI new customs parking

Fig. 3: Ancona ferry port infrastructures

Part IV

Legal Ramifications of Blockchain Technology

SECTION I

BLOCKCHAIN AND CRYPTOCURRENCIES

INTRODUCTION

KONSTANTINOS SERGAKIS

In this section, various contributors have aimed to highlight in a stimulating and interesting fashion the opportunities and challenges arising from blockchain (distributed ledger) technology.

T. Agmon and L. Cohen offer an overarching and highly interesting Analysis on the economic framework and the various applications of blockchain technology, by correctly pointing out that such technology can potentially transform the economic system in its distribution, trade and reallocation components with an overall impact on its production and consumption facets. Focusing on neoclassical exchange economy principles and providing a historical account of different monetary policies, they delve into the niceties of blockchain by emphasising its potential for further growth. The general absence of transaction costs and moral hazard make blockchain not only popular but also a truly innovative and value increasing medium of exchange. The authors predict a continuous growth of decentralised peer-to-peer trading protocols in tokens and they also opine that such growth will be primarily expressed within capital market structures. They also argue that fiat money will continue to be relevant especially in the spot market for goods and services, by leaving a continuously growing space to decentralised trading protocols. It is the authors' belief that, once such protocols expand significantly across markets, global trade and welfare will benefit in an organic and incremental way.

The remaining contributions touch upon specific issues related to blockchain: privacy, criminal, tax and raising capital features create a harmonious overarching vision of blockchain, by denoting the common denominator of different approaches which relates to the continuous effort of legal norms to grasp the reality and constantly evolving *modus operandi* of blockchain. It is not surprising that the legal order is constantly experimenting the limits of its intervention power, aiming to balance the need to safeguard the legitimate interests of recipients of such products with the objective of fostering innovation and entrepreneurship.

M. Baldi, D. Calabrese and G. Rafaiani focus on the implications of blockchain in the area of privacy, with a specific focus on confidentiality and the right to be forgotten, which is inherently contradictory to the maximum transparency that public ledger technology features. GDPR issues are dealt with in relation to various proposals that have been advanced in the literature so as to safeguard privacy prerequisites in this field. The authors correctly point out to the lack of complete immunity of systems to various potential attacks in the blockchain system and aim to provide examples of GDPR compliant systems. In parallel, they alarm the reader on the fact that the constant evolution of blockchain will continue to present challenges to the safeguard of privacy elements.

In a very interesting analysis that aims to highlight the risks arising from the use of cryptocurrencies and the response from the criminal legal order, R. Acquaroli focuses primarily on the concept of anonymity and aims to demystify the general impression that cryptocurrencies' anonymity is one of the foundations of criminal activity.

Indeed, Acquaroli argues that this statement is not entirely accurate since the real challenge is to unveil the identity of a real user of the operation, not to fight anonymity in itself. The author aims to highlight the difficulty is that criminal enforcement is faced with, also in relation to money laundering activities, and he also opines that one of the main and most preoccupying issues relevant to the enforcement agenda is the design and development of technologies for the pursuit of intrinsically illegal purposes which risk distorting entirely the operational context within which critical currencies have emerged in everyday life.

G. Rivetti and P. Cricco offer an overview of several components of the blockchain operational framework by highlighting the main features of and the underlying rationales for its success in the current era. Touching upon the wide range of cryptocurrencies, they focus on Bitcoin, Ripple and Ethereum so as to highlight the various differences as well as opportunities that these cryptocurrencies offer to market actors. Most importantly, they critically assess the fiscal regime applicable to virtual currency transactions, distinguishing between such transactions being carried out professionally and on a regular basis and transactions being held by natural persons outside their business activity. Tax issues are also relevant to money laundering and terrorist financing activities in relation to the use of cryptocurrencies; managing such challenges at the global scale is a herculean task. Rivetti and Cricco highlight the various developments in this area in attempting to link tax offences to money laundering ones, by correctly pointing out that on many occasions tax offences such as evasion may be used as an instrument to reinsert illegal funds in the economic activity or as a facilitating mechanism of criminal conduct.

Turning to the last contribution of this section, a particular focus is dedicated to capital raising operations. A. Laudonio critically assesses the somewhat disabled capacity of the legal order to adapt to constantly evolving market developments, such as those in the area of Initial Coin Offerings (ICOs). By offering a comprehensive analysis of ICOs, Laudonio proceeds with their comparison with the traditional capital market structure in terms of products, financial intermediation, disclosure obligations and supervision, and he denotes the existence of ICOs in a parallel dimension that stimulated further the search of their legal purpose. Laudonio analyses further potential common denominators between the basic components of ICOs and the ones deriving from company and financial markets law, attempting to provide some reflections in relation to their *modus operandi.*

Going beyond legal technicalities, Laudonio wisely points out that ICOs are more likely to attract retail investors, whose protection from potential abuses renders the construction of an efficient legal order of prime importance. The question then falls upon national or supranational frameworks to take the lead on providing workable and reliable environments so as to correctly address the challenges arising from new ways of raising capital while offering legal certainty to market actors, such as issuers and intermediaries. Laudonio clearly favours a supranational approach, estimating that the current initiatives at the national level that aim to create new categories of financial products or new investment services, let alone innovation hubs and regulatory sandboxes, are likely to trigger a further fragmentation of financial markets law and of a harmonised approach.

One of the main challenges of national legal frameworks in becoming champions of financial innovation and guardians of financial stability is the potential of becoming part of a supranational coordinated effort so as to create a level playing field in the applicable rules and in the expectations of all involved market actors. There is no doubt that, for such a plan to materialise, political willingness will be key in driving forward legal reforms and alignment of national to supranational standards. Waiting for further convergence efforts in this area, the authors aim to shed light on national examples that demonstrate the various challenges that the law is faced with.

THE ECONOMIC FRAMEWORK AND APPLICATIONS OF BLOCKCHAIN (DISTRIBUTED LEDGER) TECHNOLOGY

TAMIR AGMON – LEVY COHEN

SUMMARY: 1. Introduction. – 2. Trade and reallocation system in the neoclassical exchange economy with general equilibrium decentralized technology. – 3. Direct barter double coincidence of wants, neutral money, and fiat money. – 4. The new decentralized trading protocol – the media of exchange of the future. – 5. The new decentralized trading protocol – the media of exchange of the future. – 6. The potential market expansion of decentralized trading protocols. – 7. Concluding remark and a note on Bitcoin.

1. *Introduction*

The ability of individuals to trade with each other is the cornerstone of economics. Economics is a combination of three basic activities, production, distribution, and consumption. Consumption is the objective, production is what makes consumption possible, and distribution, trade, and reallocation system, is what connects production to consumption. The main research proposition of this paper is that the new innovative blockchain (distributed ledger) technology has the potential to change the distribution, trade and reallocation system, of the economic system and therefore it has the potential to change both production and consumption in a way that increases value. The new technology has the potential to change the current centralized trading (distribution) system where fiat money is the single medium of exchange to a decentralized trading system where digital cryptographic tokens that represent unique claims on current and future consumption are used as multiple media of exchange. The secondary research proposition of this paper is that it will take time and much work to develop decentralized trading protocols for segments of the markets where decentralized trading tokens that represent unique claims on current and future consumption are traded. Following Arrow (1964),[1] we believe that segments of the capital market are the best first candidates for the applications of decentralized trading protocols. The two research propositions put together deal with the economic framework and the application of the blockchain (distributed ledger) technology.

Adam Smith has suggested in his book "The Wealth of Nations" (1776),[2] a book that became the foundation for modern economics, that division of labor drives economic growth and "exchanging" (trade and reallocating system) is what makes division of labor possible. Another implication of the analysis of Adam Smith is that the nature of the trade and reallocation system is a function of the size and the nature of the market. Trade and reallocation systems can be distinguished by the way that the exchange among individuals

[1] K. J. Arrow, 'The Role of Securities in the Optimal Allocation of Risk Bearing' (1964) 31 The Review of Economic Studies 91.

[2] A. Smith, *An Inquiry into the Nature and the Causes of the Wealth of Nations* (Random House 1776).

is done. A useful distinction is among two generic trade and reallocation systems; (1) a direct person to person barter where the media of exchange are the traded goods and services, and (2) a monetary exchange where trade is executed in two steps; from a traded good or service to money (a sale) and from money to a good or a service (a purchase). Which trading system is used depends on the technology at the time. The first trade and reallocation system, the direct barter, rules until the beginning of the Industrial revolution. The second trade and reallocation system using money, the monetary system, is in operation since the beginning of the Industrial Revolution and it is associated with the tremendous growth in global trade and the growth in GDP per capita and in global population. The direct barter and the monetary exchange trade and reallocation systems are a function of market dimensions and technology. The combination of market dimensions and technology defines what Smith calls 'the extent of the market'. The main market dimensions are geography, the volume of trade, the number of participants in the trade and the variety of goods and services available for consumption. Except geography all the market dimensions depend on technology. Division of labor increases with an increase in the extent of the market. Technology brings new goods and services to the market and reduces prices. Price reductions and higher variety increase welfare increasing (Dixit and Stiglitz, 1977).[3]

The rest of the paper is comprised of the following six parts. Part 2 deals with the trade and reallocation system in the neoclassical exchange economy. This is done as the digital crypto graphical tokens traded in decentralized trading protocols represent unique claims on current and future consumption as such, they are a concrete application of the conceptual Arrow and Debreu (1954)[4] state contingent claims. Therefore, it is a proper starting point to discuss for a paper that deals with the economic framework and application of the blockchain (distributed ledger) technology. The neoclassical economic model remains a concept. There was no technology at the time that could turn the concepts of state contingent claims and complete market into practice. The fast technology developments in the second half of the 20th century and the first 20 years of the 21st century is brought a centralized trade and reallocation system based on fiat money and regulatory and enforcement institutions. A brief discussion of the need for and the development of centralized trading system is provided in part 3. The new and innovative blockchain (distributed ledger) technology makes it possible to move to a decentralized value maximizing trading system. A new decentralized trading protocol based on the blockchain (distributed ledger) technology is presented and discussed in part 4. The world is just at the beginning of applying the blockchain (distributed ledger) trading protocol. An application of the decentralized trading protocol to a specific segment in the capital market is discussed in part 5. Like in the case of any innovative technology a critical question is how fast and in what way the new technology will spread out in the world. In part 6 of the paper we provide a possible answer based on the history of the passenger trains in the UK

[3] K. Dixit and J. E. Stiglitz, 'Monopolistic Competition and Optimum Product Diversity' (1977) 67 American Economic Review 297.

[4] K. J. Arrow and G. Debreu, 'Existence for an Equilibrium for a Competitive Economy' (1954) 22 Econometrica 265.

in the 19th century and on the Edgeworth conjecture discussing the shrinking of core allocations to Walrasian equilibria. As in many cases in economics and elsewhere there is a certain degree of confusion between blockchain (distributed ledger) technology and the Bitcoin we end the paper with a brief note of Bitcoin.

2. *Trade and reallocation system in the neoclassical exchange economy with general equilibrium decentralized technology*

Almost 100 years after the publication of the Wealth of Nation, Walras (1874)[5] published a book in which he discussed the concept of general equilibrium and exchange economy. Walras assumes a world with no transactions cost and with perfect information. By the end of the 19th century the second Industrial Revolution reduced transactions cost, particularly those associated with transport and communication and changed the structure of production. In such a world it was possible to imagine an exchange economy and a trade and allocation system based on no transactions cost and perfect information. The assumptions used were not realistic then, but they allow designing a welfare maximization economy as an ideal to aspire for.

In the neoclassical exchange economy individuals are assumed to be both producers and consumers. They may be organized in households for consumption and in groups (firms) for production, but individuals are the decision makers, and they get in and out of groups as they wish at no cost. Individuals make decisions in order to maximize their utility following the common behavioral assumptions of convexity and non-satiation of demand and budget constraints arising from limits on their potential production. Given different capabilities and different preferences individuals maximize the utility of their consumption over time by buying and selling claims on current and future consumption. What drives welfare of individuals in the neoclassical exchange economy is the ability to separate production and consumption decisions. Arrow and Debreu (1954)[6] provides an axiomatic and mathematical model in which they discuss the existence and the nature of an exchange economy with competitive equilibrium in a world with no transactions cost and perfect information including perfect insight. In their model Arrow and Debreu make a number of assumptions about the markets in which production and consumption decisions are made. The most important assumption is that there is a finite number of state contingent commodities and services. Each commodity may be bought or sold for delivery at one of a finite number of distinct locations and one of a finite number of future time points.[7] Production is characterized by a non-increasing return to scale. It is impossible to have an output without an input. Given their budget constraints and market prices individuals choose their preferred consumption pattern over time by buying "Arrow-Debreu temporal and locational state contingent commodities". Given the assumptions of Arrow and Debreu, particularly perfect foresight and a known state contingent production for all the

[5] L. Walras, *Element of Pure Economics* (W. Jaffe tr, Allen and Unwin 1954, the original French edition was published in 1874).

[6] Arrow and Debreu (n 4).

[7] Ibid., 266.

finite periods in the future, there will be one-time trade and allocation. Future production and consumption are derived from this one-time trade and allocation. (The finite number of traders creates a problem with the concept of perfect competition. Aumann (1964)[8] suggests the use of continuum of traders to get over this problem).

The Arrow-Debreu trade and allocation system (allocation is done once and for all) is very elegant and it covers all possible developments in markets of goods and services through the device of state contingent claims on future consumption, but it lacks operational details. A way to get the Arrow-Debreu model closer to reality is provided by what is known as the 'sequence economy'. The idea of the sequence economy is that the long-run general equilibrium is composed of a series of short-term equilibria. It was originally discussed by Marshall (1920)[9] and then by Hicks (1939),[10] by Lindhall (1939)[11] and by Lundberg (1937).[12] The major driving force in the development of the sequence economy was the assumption that there exist different transactions costs between spot and future transactions. In this case the Arrow-Debreu one-time budget constraint is replaced by a series of periodical budget constraints that require periodical trade and reallocation. Three major results are derived in the context of the sequence economy model concerning equilibrium and trade and reallocation system: (1) there exists market clearing allocation (a core allocation), (2) the allocation is not generally Pareto efficient and it is not a general equilibrium solution (3) introducing money with nil transactions costs and no moral hazard and opportunistic behavior (i.e. decentralized money) as a medium of exchange will make the core allocation into a Pareto efficient competitive equilibrium. The sequence economy model was devised as a way to square the neoclassical exchange economy with the limits of the technology in the second part of the 20th century and the increasing role of governments and other regulatory institutions in the economy. It is a model relating to neoclassical economy, but without the requirement of general equilibrium.

3. *Direct barter double coincidence of wants, neutral money, and fiat money*

Economic historians like Maddison (2001)[13] have shown that the world was very static for the first 1800 years of the last two millenniums and the extent of the market as well as GDP per capita and the population of the world changed very little. Person to person (P2P) barter trade based on 'double coincidence of wants' was the ruling trade and reallocation system. People met in a local market and exchange goods and services. The extent of the markets was very limited. It was constrained by transportation and communication cost. People either know each other or at least they have common language and culture. They also know most of the traded goods and they could judge their quality.

[8] R. J. Aumann, 'Markets with Continuum of Traders' (1964) 32 Econometrica 39.

[9] A. Marshall, *Principles of Economics* (Macmillan & Co. 1920).

[10] J. R. Hicks, *Value and Capital: An Inquiry into Some Fundamental Principles of Economic Theory* (Clarendon Press 1939).

[11] E. Lindhall, *Studies in the Theory of Money and Capital* (Gorge Allen & Unwin 1939).

[12] E. Lundberg, *Studies in the Theory of Economic Expansion* (P.S. King & Son, Limited, 1937).

[13] A. Maddison, *The World Economy: A Millennial Perspective* (OECD 2001).

The variety of goods and services in the market was limited. Because market day was a weekly event and most participants come to the market every week there was a build-in incentive not to cheat. Trust was a function of the structure and the operations of the market. It was generated locally at the level of the community. The media of exchange were the items exchanged by the two traders involved in the exchange and they were specific to the transaction. This changed dramatically since the beginning of the Industrial Revolution at the beginning of the 19th century. By the end of the 19th century global trade reached 30% of the GDP. The extent of the market was greatly increased due to technological innovations like the transatlantic telegraph cable, the Pacific railroad and a number of innovative maritime technologies (Durkal Gun et al. 2017).[14] The ratio of exported goods to GDP (in 1913 relative prices) went up from about 7% in 1900 to 12% in 1927. The vast increase in the geography of global trade, the increase in the variety of traded goods and services and the number of people involved in trade made it less intimate and less direct than before. It was rare for the original producers of traded goods and services to meet and know their customers. Another important facet of the inventive process that begun with the Industrial Revolution is adding new, often unexpected, goods and services to the market. It also generated new production technologies. All this changes relative prices that requires periodical readjustment as is suggested by the sequence economy model and the consequent trading and reallocation system. The substantial growth of the 'extent of the market' creates a need to find a different medium of exchange. In theory there is no need to limit the number of goods and of traders in a direct barter system. Conceptually the actual goods and services traded in the market could be the media of exchange. In an article titled: "A Walrasian Theory of Money and Barter" (1966), Banerjee and Maskin say that: "[…] barter seems no worse than monetary exchanges if apples can serve as media of exchange. However, in actual markets physical goods like apples cannot be used as media of exchange as they are not uniquely defined. Each apple is different in some ways from all the other apples".[15] Yet, as the number and the variety of traded goods and services increases the condition of double coincidence of wants became extremely limiting, there was no effective technique for a series of pairwise transactions to replace the double coincidence of wants, and the variety of goods and services became too large, to rephrase Banerjee and Maskin 'all apple became different from one another'. There was a need to a medium of exchange that will separate sales of an item from the purchase of another item. Money became such a medium of exchange. The problem was and still is that money always serve as medium of exchange and as something else. The currently used fiat money is used as a medium of exchange and as a policy variable by governments and by central banks.

Economists who deal with the role of money in the economy have realized long ago that the same money cannot be used as a medium of exchange and a policy instrument. They separated in their research the role of money as a medium of exchange from the role of money as a policy instrument. Monetary economists have realized that fiat money issued

[14] D. Gun, Ch. Keller, S. Kochugovinda and Th. Wieladek, 'The End of Globalization as We Knew It?' (2017) Barclays.

[15] V. Banerjee and E. S. Maskin, 'A Walrasian Theory of Money and Barter' 1996 CXI Quarterly Journal of Economics 955.

by governments and used as the common medium of exchange is also used as a policy instrument, and as a way to extort tax from the users of money in addition to its function as a medium of exchange. These functions of fiat money interfere with its role as a medium of exchange. In a survey chapter on the transaction's role of money, Ostroy and Starr (1990)[16] present decentralized ideal money with no transactions cost, no central management and no strings attached. Such money is conceptually equal with decentralized trading protocols and it is consistent with competitive equilibrium and overall optimal assets allocation, but such money does not exist. As long as issuing money is a monopoly of governments it cannot be decentralized. In general, no single medium of exchange can be optimal if it depends on an institution like a government, or on its rarity, like gold as the person or the persons who control the quantity of the single medium of exchange have some monopoly power.

The problems and difficulties in using money as a single medium of exchange were well-known to decision makers as well. There were many efforts to find a solution. A major example was the Bretton Woods/IMF agreement that was an attempt to keep the gold standard combined with fiat money. It did not work due to opportunistic behavior of most if not all the signatories to the agreement. In the early 1970's it was replaced by a fiat money monetary exchange with the US dollar as the lead currency. In a paper titled: "The Transition from Barter to Fiat M without a "gold anchor". Ritter (1995)[17] said that the two requirements for a successful medium of exchange are standardization and credibility. A host of international organizations and agreements have tried to keep high level of standardization. Yet, more than once governments have renounced their promises for convertibility at a given exchange between fiat money and goods and services, introduce inflation, and use money as a policy instrument to achieve policy and political goals. Opportunistic behavior and moral hazard are unavoidable in a political system where human beings are making decisions. Global market with a growing market extent requires trade and reallocation system that has global standardization and global unconditional credibility. The fiat money system does not fill this bill. The developing blockchain (distributed ledger) technology heralded by the development of the Bitcoin introduces the potential of a decentralized trading and reallocation system based on trading in tokens registered on blockchains that are "approximations" of the Arrow-Debreu state contingent claims that were the building block of the neoclassical exchange economy.

4. *The new decentralized trading protocol – the media of exchange of the future*

The new and innovative blockchain (distributed ledger) technology makes it possible to accommodate the needs of an ever expanding global market, an increase in the extent of the market, and to do it in complete trust and with no opportunistic behavior and moral hazard. Decentralized P2P trading protocol operating on a blockchain is the answer to the need for an appropriate medium of exchange with no transactions cost other than minimal

[16] J. M. Ostroy and R. M. Starr 'Chapter 1. The transactions role of money', in B. M. Friedman and F. H. Hahn (eds), *Handbook of Monetary Economics* (Vol. 1, North-Holland 1990) 3.

[17] J. Ritter, 'The Transition from Barter to Fiat Money' (1995) 85 American Economic Review 134.

operations cost and more importantly with no moral hazard and other strings attached . Some basic features of blockchains (distributed ledger) technology make the new decentralized trading protocol very different from fiat money. Iansiti and Lakhani (2017) claim that "blockchain could dramatically reduce the cost of transactions. It has the potential to become the system of record for all transactions. If that happens, the economy will once again undergo a radical shift, as new, blockchain-based sources of influence and control emerge".[18] Lasiti and Lakhani identified five components of the blockchain technology that are both enablers and necessary features for a decentralized trading protocol. The five features are:

- distributed database,
- P2P transmission,
- transparency with pseudonymity,
- irreversibility of records,
- computational logic that eliminates most of the transaction costs, including moral hazard.

Given these features blockchain technology makes it possible to provide an efficient way to enable universal P2P barter trading in tokens registered on blockchains where the tokens represent claims on current and future consumption. Unlike the conceptual Arrow-Debreu state contingent claims the claims traded by decentralized trading protocols are tokenized assets. The tokens are claims held by individuals as representations of real assets in a similar way that securities represent real assets. Following the model of an "exchange economy" we assume that trade is taken place among assets holders who exchange tokens among themselves. Such a trade model is described and discussed in Aumann (1964)[19] and applied in Given blockchains and P2P decentralized trading protocol it is possible to execute quickly a long series of pairwise transactions such that traders will be able to exchange the tokens that they own with the asset (tokens) that they want. The trading protocol for tokenized assets issued on blockchains allows doing that in a completely trusted and verifiable way and tokens become the media of exchange.

There are three necessary conditions that make decentralized trading protocols possible:

a) The ability to issue cryptographic tokens on public or private blockchains.
b) An ability to issue digital cryptographic tokens representing claims on current and future goods and services (physical goods and services and promises to provide goods and services in the future). The tokens should be uniquely defined such that two tokens on the same good or service are interchangeable.
c) A decentralized trading protocol that will allow exchange of a series of pairwise transactions and will eliminate the opportunistic behavior associated with centrally managed money like fiat money. Such protocols exist in various stages of development.

Condition (a) does exist today. Cryptographic digital tokens can be issued on public and on private blockchains. What prevents a broad applicability of decentralized P2P

[18] M. Iansiti and K. R. Lakhani, 'The Truth About Blockchain' (2017) Harvard Business Review <https://hbr.org/2017/01/the-truth-about-blockchain>.

[19] Aumann (n 8).

barter is the inability to issue tokens against most goods and services available in the market, (condition (b). This is so because most assets traded in the global market are not uniquely defined and therefore it is not possible to issue a cryptographic digital token against them and to register the token on a blockchain. Therefore, we limit the discussion of the application of decentralized P2P barter trading to specific segments of the capital market where the assets are uniquely- defined. This is a first step. Once the decentralized trading protocol will be applied successfully to relatively small segments of the capital market it is likely that more applications will follow. Such a process is discussed in section 4 below. Condition (c) is "in the making". Decentralized trading protocols exist although they are not fully operational as yet.

5. *Applying a P2P decentralized trading protocol to a segment of the capital market*

In this section we set up a model of a defined contribution (DC) pension plan to demonstrate in what way decentralized P2P barter trading described and discussed in section 2 above increases the value of beneficiaries in the DC pension plan outlined below.

Assume a DC pension plan where a group of beneficiaries enter into a contract with a management company to invest in and manage a portfolio of assets. We assume that management can invest the money only in financial assets traded on public markets and that the management group has no influence, control or management rights in the companies in which the management of the pension plan invests. The beneficiaries invest as a group an amount of V at t=0. The share of each beneficiary in the assets of the DC pension plan at t+0 is proportional to her/his share in the overall initial investment. Once the money is invested and the DC pension plan has a portfolio of publicly traded financial assets, e.g. shares, bonds, options and such like, the management issues tokens per each asset on the blockchain and distribute them proportionally to the beneficiaries. Issuing the tokens is possible as the assets held by the DC pension plan are well-defined being because they are purely financial claims. It is possible to look at the issuing and distribution of the token as if the beneficiaries issue the tokens against their claims on the assets of the DC pension plan. Once the tokens are registered on the blockchain they are in the wallet of the beneficiaries and they can trade among themselves in the tokens that they received provided that at the end of the trade all the beneficiaries hold all the tokens. The tokens are good as long as management does not change the portfolio of securities held by the pension plan. Any time that management adjusts the portfolio the process of issuing and distributing tokens repeats itself given the previous holdings of each beneficiary. At t=n the last period in the contract between the management and the beneficiaries the management distribute the assets (or their value) to the beneficiaries according to the tokens they hold at t=n. The prices in which the tokens are traded are determined by the market price of the assets that the tokens represent. For simplicity we assume that at any period there is a limited specific time in which trade can take place. In this we follow what is known as the 'sequence economy'. The idea of the sequence economy is that the long-run general equilibrium is composed of a series of short-term equilibria. In this case the Arrow-Debreu one-time budget constraint is replaced by a series of periodical budget constraints that require periodical trade and reallocation. Three major results are derived in the context of the sequence economy model relative to the trade and reallocation system: (1) there exists market clearing allocation (a core allocation), (2) the allocation is not generally Pareto efficient, and (3) introducing money with nil transactions cost and no moral hazard as a global medium of exchange will make the core allocation into a Pareto efficient competitive equilibrium. In our example the decentralized trading protocol acts as the ideal money with nil transaction costs and no opportunistic behavior and moral hazard. Hence, the outcome of the periodical internal trading in the pension plan is Pareto optimal for the beneficiaries with respect to their holding in the pension plan. Trade is executed only where some beneficiaries within the group are willing to exchange token held by them with tokens held by others in the group. The above mechanism is similar to the Fama-Miller describe as the case where an investor issues a claim in period 1 against a fragment of a value distribution in period 2 issued by a firm. In our case the investor is a beneficiary in the pension plan and the company is the management of the pension plan.

The outcome of the internal trading within the pension plan is a core allocation among the beneficiaries. Our example follows Aumann (1964)[20] description of a core allocation where the number of traders is small relative to the population at large. Aumann says that: "The market model that we consider consists of a set of traders, each of whom starts out with an initial commodity bundle to be used for trading, and each of whom has a well-defined preference order on the set of all commodity bundles. A trade (or allocation) is a redistribution of the commodities in the initial bundle among the traders".[21] The prices, or the allocation among the members of the group, are not a competitive equilibrium price. As Aumann says: "An allocation x is said to be in the core of the market if no coalition of traders can force an outcome that is better than for them than x".[22] Prices in a core allocation are determined in trade among the members of the group. The number of the traders in the group can be very small relative to the market at large. It is shown in section 4 below that core allocations are a necessary stage in the adjustment of the market to new processes like new exchanging.

6. *The potential market expansion of decentralized trading protocols*

History of game changing technologies as well as economic theory provides us with clues for how the blockchain (distributed ledger) decentralized trading protocol may develop as a value increasing medium of exchange. We begin this section by looking at the expansion of the steam railway in England and generalize the process by looking at the core convergence process. The early development of the steam powered railway in England provides relevant information to the way that transformational technologies like the blockchain and distributed ledger technology may develop. The development of the railway is of particular interest as it can be seen as a technology that connects between the production and the consumption and it is an important part in the process of "exchanging"

[20] Ibid.

[21] Ibid.

[22] Ibid.

discussed at the beginning of this paper. Prior to the introduction and the development of the steam powered railway people hardly travel more than 10 miles from the place in which they were born and their ability to develop and trade their assets including their time and capabilities was very limited. Still it took time to realize the potential of steam powered trains to increase the value of assets, time and capabilities of individuals through trade. The steam engine that makes steam powered trains possible were developed in 1776 and it took more than thirty years until the 25 miles' line from Stockton to Darlington was built. The purpose of this line was very limited; to transport coal from the source of the coal to the users. The real contribution of steam powered trains came from passengers. In 1830 the first intercity train connection was built to connect Manchester and Liverpool. Ten years later, in 1840, there were 20 million passengers' journeys per year. In 1911 the number of journeys went up to 1.3 billion. In less than 100 years what has begun as providing better transportation services for short hauls of the coal industry in England turns into a major facilitator of economic growth in England and in the world.

The brief history of the development and the contribution of the steam powered railway in England provide a historical perspective of the potential development of what turned to be a game changing technology. The use of decentralized trading protocol as value increasing medium of exchange may begin with applications to relatively small segments of the capital market like the DC pension plan discussed in section 3 above. But this is likely to be only a first step in a process of generating more and more applications. The limited initial applications can be seen as limited core allocations with a potential for replication.

The example of the DC Pension Plan discussed above deals with a limited segment of the capital market. It affects only a part of the assets of the beneficiaries of the DC pension plan who may have assets outside their share in the plan. Yet, creating a core allocation where trade is taking place using a decentralized trading protocol is an important first step. Core allocations may be very small, but they often start a process that leads to optimal assets allocation for larger groups of people and cover a larger part of the market.

Edgeworth conjecture, 1883, hypothesizes that the core of the economy shrinks to the Walrasian equilibria as the number of agents increases to infinity. Debreu and Scarf (1963)[23] offer a formal proof to the Edgeworth conjecture. In their Core Convergence Theorem, they assert that for economies with a large number of agents, core allocation is "approximately competitive". We suggest that as more and more claims on current and future goods and services will be sufficiently uniquely defined such that it will be possible to issue cryptographic tokens against them, the rate of use of decentralized P2P trading protocol in tokens will grow. It is likely that the development and the growth of decentralized trading protocol using tokens as media of exchange will focus on the capital market. Fiat money will continue to be a medium of exchange, particularly in the spot market for goods and services. As long as decentralized trading protocols will be available only for trade in a very limited and marginal assets total volume of such trade will be very small. Traders may opt to use money as a medium of exchange even for assets that could

[23] G. Debreu and H. Scarf, 'A Limit Theorem on the Core of an Economy' (1963) 4 International Economic Review 235.

be traded through decentralized protocol because they would not bother to move from what they have done before and engage in a new form of trading for a very small part of their trade. But as the share of trade that can be done through decentralized trading protocol will go up and more traders will move to the new and more effective trading mode the economy will become, to use a term coined by Debreu and Scarf, "approximately competitive".

7. *Concluding remark and a note on Bitcoin*

To some extent the bitcoin became synonym with the blockchain (distributed ledger) technology. This is misleading. The bitcoin is a currency that was issued on and with the help of specific blockchain. The purpose of the bitcoin is to maintain value and allows a transfer of value among holders of bitcoin on a blockchain. The main incentive for the development of the bitcoin was to create decentralized money free of government's intervention. It is a store of value and not a medium of exchange. What we do in this paper is to discuss an application of a decentralized trading protocol for multiple parties through multiple media of exchange. The decentralized trading protocol makes it possible to have a multiple parties, multiple goods and services trade that does not use fiat money as a single medium of exchange. We have shown that such a trading protocol once extended to a large enough segment of the market will increase serve global trade well and will increase economic welfare in the world.

BLOCKCHAIN AND PRIVACY: CAN THEY COEXIST?

MARCO BALDI – DALILA CALABRESE – GIULIA RAFAIANI

SUMMARY: 1. Introduction. – 2. Privacy requirements of technological infrastructures. – 3. Blockchain technology. – 4. Privacy-preserving blockchain architectures. – 5. Security analysis. – 6. Conclusion.

1. *Introduction*

In our digitalized world, the dematerialization of documents has completely changed their conception, creation, and conservation. In the last thirty years, physical supports to produce and preserve data have been abandoned, due to the rising of digital technologies, which reduce production costs and storage spaces and increase the availability of documents. Nowadays, large amounts of heterogeneous data are continuously used, transmitted, and processed. Among those data, particular attention must be paid when subjects' personal and sensitive data, as those related to their health state, are collected, stored, and treated. Data sharing and interoperability, in fact, are the key concepts to ensure an efficient healthcare system. At the same time, the citizen who meets health facilities must be guaranteed the most absolute confidentiality and the widest respect for his fundamental rights and dignity. In Europe, the treatment of patients' data is strictly regulated by the Regulation (EU) 2016/679, the so-called General Data Protection Regulation (GDPR).[1] Health data are those "related to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his or her state of health" (Art. 4 GDPR). All data, especially health data, require transparency, security, privacy, integrity, and non-repudiation. In a context of increasingly complex and extended information systems, the blockchain represents an element of innovation. It provides an undeniable and secure architecture for storing, certifying, and sharing data. The blockchain keeps data in an immutable public transaction ledger, making it impossible to modify or delete them once entered in it. Being the ledger public, the concept of confidentiality fails. Therefore, the blockchain turns out to be intrinsically in contradiction with the GDPR prerequisites; the confidentiality or the right to be forgotten seems not to be guaranteed within it. In the literature, several approaches for creating a GDPR-compliant blockchain-based model have been proposed. In this paper, these approaches are synthesized and analyzed. Then, two GDPR-compliant abstract paradigms are proposed, to provide a synthetic abstraction of their structures and working principles. These systems provide GDPR-compliant technical solutions for the digitalization, preservation, and sharing of dematerialized data, ensuring data authenticity, validity, and interoperability. Although the technology on which the analyzed models are based seems to provide infallible and secure data exchange

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

systems, it is not immune to emerging and sophisticated attacks that can produce enormous and irreparable damages, not only in terms of privacy but also in terms of treatment effectiveness. Therefore, for each considered model, a security analysis of its privacy-preserving protocols is also carried out, to understand whether there are GDPR-compliant blockchain-based solutions able to provide secure data storage.

2. *Privacy requirements of technological infrastructures*

The GDPR, enforced in the European Union since May 2018, was introduced to standardize the privacy legislation across the European Union and to give people greater control over their personal data. The GDPR is founded on the concepts of privacy by design and privacy by default. In particular, Art. 25 of GDPR obliges the data controllers to implement technical and organizational measures capable of ensuring compliance with the principles of the Regulation, such as transparency of data processing, data minimization, storage limitation in terms of time, consent, and integrity and confidentiality of personal data. This underlines that both system design and organizational measures should account for data protection principles, rights, and obligations. The GDPR, if compared to the previous European directives, guarantees more rights to data owners; among these, the *right to rectification* (data subjects have the right to obtain the correction of their personal data in case of inaccuracy or incompleteness), the *right to erasure* or *right to be forgotten* (data subjects are entitled to request data controllers to delete their personal data), the *right to access* (the data subject is authorized to know if, for what purpose, by whom, where and how his own data are processed), and the *right to be informed* (organizations must provide information on the data processing activities in a clear, concise and intelligible manner).[2] The development of emerging technologies such as blockchain, artificial intelligence, and cloud computing will be strongly influenced by the GDPR. These technologies, considered as effective means to increase performance and productivity, offer their potential value through huge amounts of data and algorithms. Therefore, stricter data management and processing rules are slowing down their development. Since many cybersecurity incidents and data breaches happened in the past, the GDPR also requires companies to implement reasonable data protection measures to protect users' personal data against data exposure or loss and threats or violations. Among the key changes introduced with the GDPR, there is the breach notification: data controllers must inform the Supervisory Authority of any data breach within 72 hours from when they became aware of it. The users, within the same period, must be informed of the violation unless the violation is not risky for the user rights and freedoms.[3] The GDPR requires companies to make an internal evaluation of their technological infrastructures and data architecture, to be able to guarantee all the users' rights.[4] The regulation, in fact, imposes high requirements for data controllers and data

[2] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (1st ed., Springer 2017); 'What is the GDPR? A complete guide on everything you need to know to comply' <https://www.iubenda.com/en/help/5428-gdpr-guide>.

[3] Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (2019).

[4] He Li, Lu Yu and Wu He, 'The Impact of GDPR on Global Technology Development' (2019) 22 Journal of Global Information Technology Management 1.

processors and for the processing and storage of personal data. Therefore, the way data controllers and data processors handle data has radically changed: data protection is no longer seen as an additional component of the organizations but becomes an integral part of the organization itself.

3. *Blockchain technology*

The blockchain technology is a distributed ledger technology, aimed to both protect data integrity and individual freedom and to simplify the secure exchange of information and assets.[5] This shared, public, and immutable data structure is organized in blocks; each block is linked to the previous one, through a reference to it and contains records of a particular event associated with a time instant (timestamp). To obtain a growing list of validated records, each new block is verified through the computation of the digest of a one-way cryptographic function known as *hash function*, and so it is uniquely identified by a fixed cryptographic hash. Each block contains its cryptographic hash digest and the hash digest of the previous one, except for the genesis block that is created from scratch.

The blockchain infrastructure is: *distributed* (information is replicated over multiple nodes in the network), *immutable* (contents cannot be modified or deleted without corrupting the entire structure), *transparent* (the blockchain is an open file with a full transaction history), and *consensus-driven* (works without the presence of a central authority).[6] With the blockchain, in fact, there is a shift from a rigorously centralized logic, characterized by the recognition of an authority and thus by a one-to-many relationship, to a complete distributed logic based on the concept of consensus, i.e. trust among all participants or nodes. Every single node shares the archive of the entire blockchain and so every block containing transactions. A transaction is an elementary data record originally designed to represent the transfer of a digital asset from one user to another and is collected in a block of transactions. This realizes an unmodifiable exchange of information among users. Each transaction is validated by the network through a trust model based on group consensus protocols. Each block of transactions is validated by the network through a process requiring a considerable consumption of resources (usually computing power) and then added to the blockchain. At the structural level, each block consists of a timestamp, a random number (nonce), the hash of the previous block, and a list of transactions occurred since the previous block; in this way, a persistent, increasing, and constantly updated chain is created.[7]

The main protocol for the validation of blocks (also called mining) is the so-called *Proof-of-Work* (PoW): validating nodes (also called miners) continuously try to solve a cryptographic puzzle based on a hash function or similar functions. Miners who find a valid solution are then rewarded through a digital asset known as cryptocurrency. Other types of consensus algorithms are:[8]

[5] M. Pilkington, 'Chapter 11: Blockchain technology: principles and applications', in F. X. Olleros and M. Zhegu (eds), *Research Handbook on Digital Transformations* (Edward Elgar Publishing 2016).

[6] K. Sultan, U. Ruhi and R. Lakhani, 'Conceptualizing Blockchains: Characteristics & Applications' (2018) 11th IADIS International Conference Information Systems 49.

[7] G. Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger* (2014).

[8] 'What is Consensus, and how to achieve it in a Blockchain ecosystem' (7 April 2018) The Blockchain lion <https://blockchainlion.com/consensus-blockchain/>.

- *Proof-of-Stake*: suitable for contexts with low computing power, distributes the right to mine according to the amount of cryptocurrency owned by miners.
- *Round Robin*: permits miners to create a finite number of blocks, in rotation, preventing the problem of mining monopolization.
- *Practical Byzantine Fault Tolerance* (PBFT): each node signs the transaction validating the correctness of the record and sends its response to all the other nodes. The opinion of each node is published, and the status supported by more than two-thirds of the nodes is seen as the correct one.

From an administrative and an implementation point of view, different types of blockchain can be identified:[9]

a) *Permissionless Public*: anyone can control the activity of anyone, everyone can join or leave the network and participate in consensus. Read and write access is guaranteed to anyone: minimum trust is required among nodes, thus achieving maximum transparency.
b) *Permissioned Public*: there is a partial decentralization of the network. Everyone can read but writing and participation in consensus are allowed only according to some privileges granted by a group of administrators.
c) *Permissionless Private*: sharing of information does not happen publicly. Everyone can join or leave the network at any time. Decentralized algorithms on these networks establish who has both read and write access to the blockchain.
d) *Permissioned Private*: data storage occurs through a permissioned access control system managed by users of the network. The network administrators ensure network membership, providing participants with read and write access to data according to their privileges.

4. *Privacy-preserving blockchain architectures*

The blockchain, thanks to its immutability, transparency, verifiability, and resilience, offers a radically different approach to data protection if compared to centralized systems. Data protection is built over three basic pillars: confidentiality, integrity, and availability. Confidentiality is the ability to protect data not allowing unauthorized individuals to access the information. Integrity is the ability to prevent data modification in an unwanted manner. Availability refers to the possibility of accessing data when required. The blockchain architecture allows the fulfilment of both integrity and availability but clashes with the concept of confidentiality.[10] Indeed, confidentiality cannot be preserved in a public blockchain, where all the entered data are in clear and each node has a complete copy of the ledger. Moreover, once data are stored on a blockchain, they cannot be deleted or modified; this feature clashes with the right to be forgotten provided by the GDPR. It is important to understand how the blockchain immutability can be adapted to the GDPR. For example, data erasure can be implemented in different ways. One solution is to encrypt the personal information written on the blockchain, such that the destruction of encryption keys will ensure the

[9] Z. Zheng and others, 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends' (2017) IEEE 6th International Congress on Big Data 557.

[10] A. Ali and M. Mazhar Afzal, 'Confidentiality in Blockchain' (2018) 7 International Journal of Engineering Science Invention 50.

non-accessibility to that information.[11] Another possible solution is to provide proof of integrity by writing only the hash digest of data in the blockchain, while storing the data outside of it, adding the possibility to delete data. We considered different protocols found in the literature and grouped them in two basic paradigms to provide a synthetic and clear abstraction of the complex structures and working principles of the existing GDPR-compliant blockchain-based solutions. The right to be forgotten is usually faced using multiple cryptographic protocols. Data confidentiality can be ensured by storing hashes in the blockchain and putting data in a local storage outside the blockchain or by using a cryptographically manipulated version of the data.[12]

The first paradigm found in the literature is the on-chain hash/off-chain data: the hash value of the data is inserted in the blockchain, while the data are saved in a local storage. This process generates a blockchain transaction including the hash digest of the data to be stored on the blockchain, and a reference to the actual data stored in an off-chain data repository useful to guarantee the non-alteration of data at the source. This paradigm preserves data confidentiality by storing in the distributed ledger not the clear data, but their hash digests only.[13] It can be applied to both permissionless blockchains, as happens in BlocHIE[14] and MyHealthmyData (MHMD)[15] and to permissioned blockchains, as happens in Blockchain-based eHealth Integrity Model (BEIM)[16], Blockchain based Personally Identifiable Information Management System (BcPIIMS),[17] and MediChain.[18]

According to a second paradigm, confidentiality is guaranteed by entering in the blockchain not the clear data, but an encrypted version of them, obtained through a public or private key encryption. This paradigm ensures not only compliance with the GDPR, control of data access, and the guarantee that the data will not be stolen, but also pseudonymization, privacy, integrity, accountability, and security.[19] Examples of

[11] A. Al Omar and others, 'MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data' (2017) The 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage 534.

[12] G. Drosatos and E. Kaldoudi, 'Blockchain Applications in the Biomedical Domain: A Scoping Review' (2019) 17 Computational and Structural Biotechnology Journal 229.

[13] A. Bayle and others, 'When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry' (2018) IEEE/WIC/ACM International Conference on Web Intelligence 788.

[14] Sh. Jiang and others, 'BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange' (2018) IEEE International Conference on Smart Computing 49.

[15] E. Morley-Fletcher, 'MHMD: My Health, My Data' (2017) myhealthmydata.eu <http://www.myhealthmydata.eu/wp-content/uploads/2018/05/EuroPro_paper_04.pdf>.

[16] T. Hyla and J. Pejaś, 'eHealth Integrity Model Based on Permissioned Blockchain' (2019) Future Internet 76.

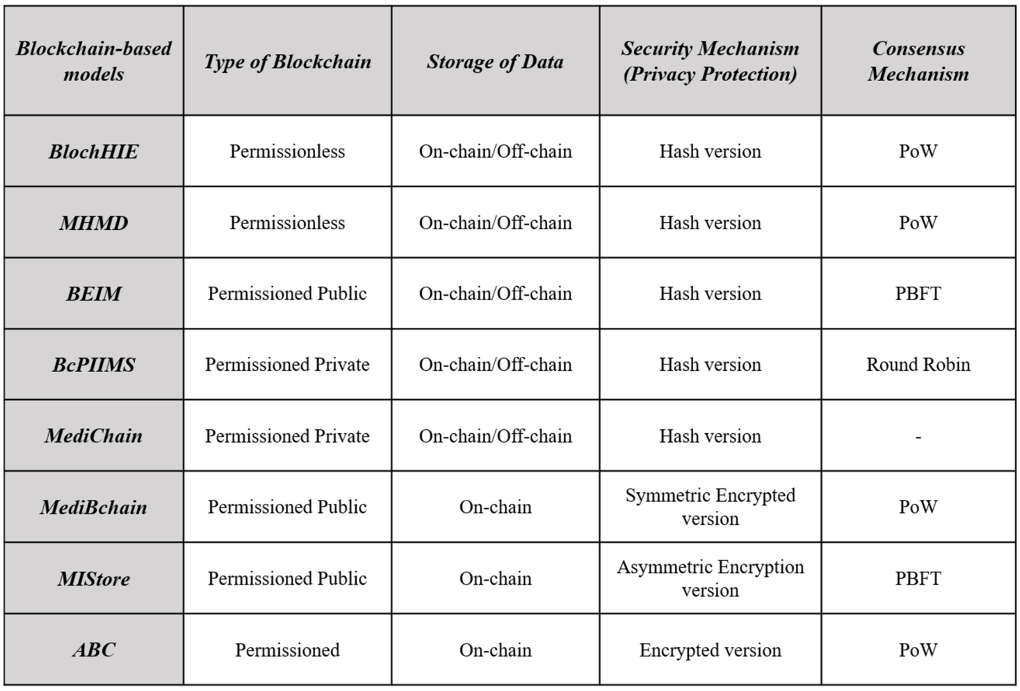
[17] N. Al-Zaben and others, 'General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management' (2018) International Conference on Computing, Electronics & Communications Engineering (iCCECE) 77.

[18] S. Rouhani and others, 'MediChain^{TM}: A Secure Decentralized Medical Data Asset Management System' (2018) IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics 1533.

[19] Al Omar (n 11).

blockchain-based models that use this paradigm are MediBchain,[20] MIStore,[21] and Advanced-Block Chain (ABC).[22]

The core technology components of each blockchain-based model mentioned above are synthesized in Table I. To be noted that all the considered models manage to guarantee integrity, confidentiality, and right of erasure.



Blockchain-based models	*Type of Blockchain*	*Storage of Data*	*Security Mechanism (Privacy Protection)*	*Consensus Mechanism*
BlochHIE	Permissionless	On-chain/Off-chain	Hash version	PoW
MHMD	Permissionless	On-chain/Off-chain	Hash version	PoW
BEIM	Permissioned Public	On-chain/Off-chain	Hash version	PBFT
BcPIIMS	Permissioned Private	On-chain/Off-chain	Hash version	Round Robin
MediChain	Permissioned Private	On-chain/Off-chain	Hash version	-
MediBchain	Permissioned Public	On-chain	Symmetric Encrypted version	PoW
MIStore	Permissioned Public	On-chain	Asymmetric Encryption version	PBFT
ABC	Permissioned	On-chain	Encrypted version	PoW

Table I: Core technology components of the analyzed GDPR-compliant blockchain-based systems

5. *Security analysis*

Different types of attacks have been considered to assess the security of the previously described paradigms and models:

a) *Network-based attacks*
   - *Replay Attack* – the executor intercepts and retransmits the original message within a network. Because of the validity of the original data, which come from an authorized user, the attack is treated as a normal data transmission. A replay attack is favored in blockchains based on PoW consensus mechanism.[23]
   - *Sibyl Attack* – an attacker could impersonate multiple distinct identities to subvert the integrity of the network by increasing its own voting power. In blockchain-based models that use PoW, the creation of a new identity implies

[20] Ibid.

[21] Lijing Zhou, Licheng Wang and Yiru Sun, 'MIStore: a Blockchain-Based Medical Insurance Storage System' (2018) 42 Journal of Medical System 149.

[22] W. Liu and others, 'Advanced Block-Chain Architecture for e-Health Systems', in *19th International Conference on E-health Networking, Application & Services (HealthCom): The 2nd IEEE International Workshop on Emerging Technologies for Pervasive Healthcare and Applications* (ETPHA 2017).

[23] M. Saad and others, 'Exploring the Attack Surface of Blockchain: A Systematic Overview' (6 April 2019) arXiv preprint 1904.03487 <https://arxiv.org/abs/1904.03487>; M. Vukolić, 'The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication' in J. Camenisc and D. Kesdoğan (eds), *Open Problems in Network Security* (Springer 2016).

the addition of computing power to solve the cryptographic problem, thus making Sybil attacks expensive for opponents.

- *Distributed Denial of Service (DDoS) Attack* – many malicious machines are directed to target a single network node aiming to overload it with a massive amount of traffic to produce a network congestion. In systems based on the PBFT mechanism, this attack could be more feasible than in those that use other consensus mechanisms, since the attacker needs to have control over only the 33% of the nodes to mount the attack.[24]

b) Mining-based Attacks

- *Majority Attack (or 51% attack)* – occurs if a miner or mining pool alone manages 51% of the network power, allowing him to make invalid transactions, prevent verification, allow double-spending, split the network, or fork the main blockchain. The models based on consensus mechanisms different from PoW, which are not based on heavy computational tasks, are considered less robust against this attack.[25]
- *Selfish Mining Attack* – is led by a miner with more than 25% of the total computing power who manages to secretly validate a block before the others, building a hidden chain. When the selfish miner reveals his private chain, demonstrating more PoW compared to other miners, he achieves greater rewards. It is an attack specific to blockchains based on a PoW consensus mechanism.[26]

c) Security mechanism-based Attacks

- *Brute Force and Dictionary Attacks* – attempt to invert the hash function, trying every possible combination of the input (brute force) or trying a reduced set of inputs that are likely to work (dictionary). Those attacks apply to all the protocols that store a hash digest on a public blockchain.
- *Overload Attack* – exploits the redundancy of the system and its correlated low efficiency. The most sensitive structures to this attack are those that preserve data with an on-chain storage and the models that use PBFT.
- *Padding Oracle Attack* - uses cryptographic message filling or padding validation to decrypt a ciphertext; indeed, this attack affects the models that use encrypted data storage in the blockchain.[27]

Combining the technical components of each blockchain-based model and the characteristics of every attack, it is possible to obtain a picture of the risk related to the use of each GDPR-compliant model. The results of such a security analysis are schematically summarized in Table II. It is possible to observe that none of the considered GDPR-compliant blockchain-based models is totally immune to the whole

[24] Saad (n 23).

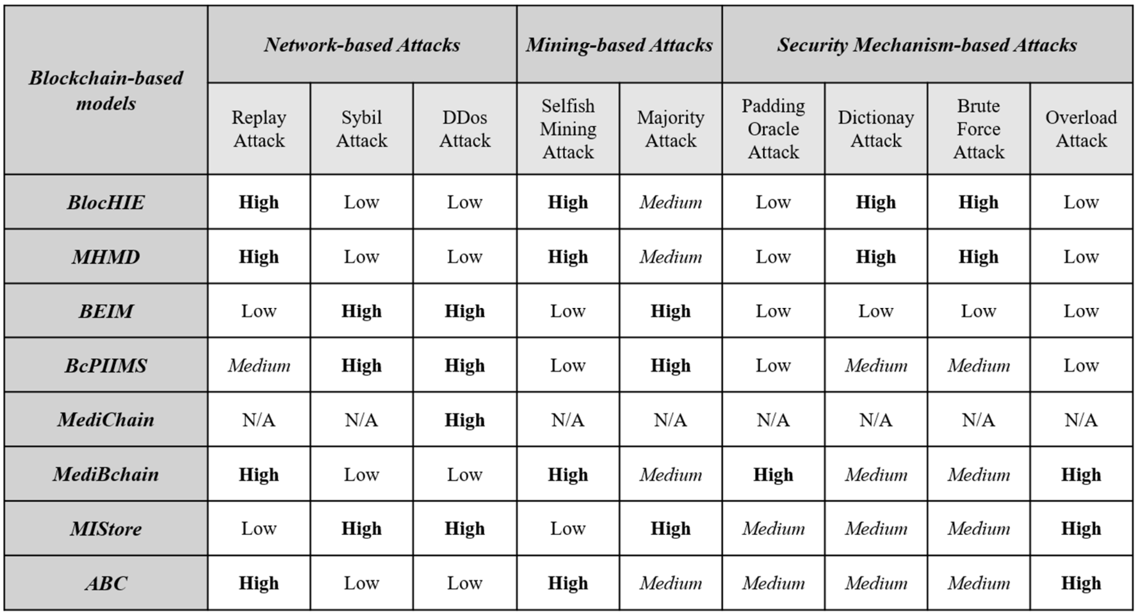
[25] Ibid.

[26] M. Saad and others, 'Countering Selfish Mining in Blockchains' (2018) arXiv preprint 1811.09943 <https://arxiv.org/abs/1811.09943>.

[27] James Manger, 'A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0' in Kilian J. (eds), *Advances in Cryptology - CRYPTO 2001* (Springer 2001).

set of considered attacks. The consensus mechanism is a discriminating factor in the assessment of the applicability of the considered attacks. The analysis of the results shows that the most promising solutions are those that, to comply with the GDPR, combine a permissioned blockchain with a consensus mechanism different from PoW. However, the use of a consensus mechanism different from PoW exposes these systems to the risk of Sibyl attacks. The susceptibility of the PBFT mechanism to Sybil attacks could be solved by increasing the number of nodes of the network, since a low number of nodes facilitates this attack. However, the increase in the number of nodes leads to scalability problems, since models based on the PBFT mechanism work efficiently with a small consensus group. Therefore, a trade-off should be found. It is also worth observing that, among the solutions that use PBFT in a permissioned blockchain, those that preserve data by combining an on-chain/off-chain storage using a hash computation are immune to Overload and Padding Oracle attacks.

It is possible to conclude that, among the considered models, the most secure are those exploiting a permissioned blockchain based on a consensus mechanisms different from PoW, like PBFT, and which use the combination of on-chain and off-chain storage through hash computation.



Blockchain-based models	***Network-based Attacks***			***Mining-based Attacks***		***Security Mechanism-based Attacks***			
	Replay Attack	Sybil Attack	DDos Attack	Selfish Mining Attack	Majority Attack	Padding Oracle Attack	Dictionay Attack	Brute Force Attack	Overload Attack
BlocHIE	**High**	Low	Low	**High**	*Medium*	Low	**High**	**High**	Low
MHMD	**High**	Low	Low	**High**	*Medium*	Low	**High**	**High**	Low
BEIM	Low	**High**	**High**	Low	**High**	Low	Low	Low	Low
BcPIIMS	*Medium*	**High**	**High**	Low	**High**	Low	*Medium*	*Medium*	Low
MediChain	N/A	N/A	**High**	N/A	N/A	N/A	N/A	N/A	N/A
MediBchain	**High**	Low	Low	**High**	*Medium*	**High**	*Medium*	*Medium*	**High**
MIStore	Low	**High**	**High**	Low	**High**	*Medium*	*Medium*	*Medium*	**High**
ABC	**High**	Low	Low	**High**	*Medium*	*Medium*	*Medium*	*Medium*	**High**

Table II: Results of technical analysis of security vulnerabilities in terms of risk (N/A = Not Applicable)

6. *Conclusion*

The immutability and the public and distributed nature of the blockchain seem to be in contradiction with the GDPR requirements. However, several solutions based on different storage mechanisms have been proposed to guarantee data confidentiality, integrity, and availability while using blockchain-based infrastructures. According to our analysis of the vulnerabilities of several GDPR-compliant blockchain-based models, the use of permissioned blockchains based on a consensus mechanism different from PoW and exploiting an on-chain hash/off-chain data management paradigm appears to be the best suitable one for ensuring both security and compliance with the GDPR.

BLOCKCHAIN AND CRIMINAL RISK

ROBERTO ACQUAROLI

SUMMARY: 1. Why criminal law has dealt with blockchain. – 2. Criminal alarm for the use of cryptocurrencies. – 3. Anonymity as a crime? – 4. Conclusions.

1. *Why criminal law has dealt with blockchain*

In the last decade, also criminal law had to deal with the world of virtual currencies, more precisely, cryptocurrencies that exploit the technology and the potentialities offered by Blockchain. Blockchain is a protocol capable of certifying the chronological order of a series of operations, using a single chain of blocks or algorithms in which each subsequent transaction or operation is indelibly and irreversibly linked to the previous operations. In particular, the characteristic of this technology, from which the problematic nature of the "classic" criminal law approach derives, consists in the presence of a linked series of blocks, which record, for each operation, the identity of the payer, the amount transferred and the identity of the beneficiary: "Each block contains information related to transactions carried out consecutively over a period of ten minutes, as well as a reference to the previous block. In this way, the Blockchain provides a complete and updated representation of all the transactions that have taken place since the system was started up to that moment".[1]

Starting from the last decade, a series of decentralized and convertible crypto currencies have been triggered on this technology, among which the most famous is Bitcoin, which represent a sort of realization of an unprecedented perspective, as regards the traditional monetary system. In fact, Bitcoin creates a sort of "financial democracy", characterized by the absence of intermediaries and state control, which would have, as its objective, the creation of an economy and a "totally free market, whose regulation is exclusively delegated to individual participating users of the system".

The same philosophy which animates the creation and dissemination of virtual currencies, therefore, appears to be in contrast with the existing system of order in matters of governance of the currency and financial markets. In fact, it expresses its *raison d'être* "in the equality of conditions among all individuals", which excludes the presence of a *super partes* body that controls its work, in the absence of rules that slow down the deliberately rapid and left to the exclusive decisions of individual actors. It is therefore an economic dimension that theorizes the trust that the individual user places in the other operators of the blockchain, whom we do not know the name, but only the encrypted code. This is a particularly delicate issue with regard to virtual currencies, such as bitcoin, in which "each person holding a bitcoin account is

[1] F. Di Vizio, 'Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti' (2018) Diritto penale contemporaneo 21 <https://archiviodpc.dirittopenaleuomo.org/d/6224-le-cinte-daziarie-del-diritto-penale-alla-prova-delle-valute-virtuali-degli-internauti>.

guaranteed total confidentiality about her/his identity, so that the user can preserve both privacy from state control relating to his own person, as well as that relating to the object of her/his own sales".[2] It should also be noted that, in this regard, it is more appropriate to speak of "pseudo anonymity" since each transaction, which took place in crypto currency, is actually recorded in a sort of digital ledger (distributed ledger) in the public domain, accessible by anyone, from which it is possible to trace part of the operation carried out in the blockchain to the accounts.

The diffusion of crypto currencies could not fail to draw attention to their possible use for illegal purposes, given the purely economic nature of the transactions carried out; and, above all, the connotations that characterize it. In particular, there are three features of the blockchain system that have repeatedly drawn attention to the risk of its use for illegal purposes namely:

a) the anonymity or pseudo anonymity of users of cryptocurrencies;

b) the virtual environment in which crypto currency develops and feeds a very dense series of exchanges: the network, in fact, allows transactions to be carried out in a very short time at an international and transnational level, exploiting, precisely, the possibilities offered by the web, on a par with what happens for any other form of economic and financial relationship of the so-called legal economy;

c) the singular and complex structure of the blockchain, which feeds the suspicion of illegal operations;

d) the absence, or better, the choice to avoid any form of regulation and control by the authority. The feature is considered both as an obstacle to the prevention of economic and financial crime phenomena, connected not only to white-collar crime, but also to organized crime and international terrorism; both as an indication of suspicion of illegal conduct, aimed not only at hiding the movements of money, but rather at the use of virtual money, once converted into real money, in illegal transactions.

2. *Criminal alarm for the use of cryptocurrencies*

Criminal literature has for some time highlighted the risk that cryptocurrency is a suitable, if not privileged, instrument for operations of an illicit nature, especially in relation to money laundering phenomena, attributable to cyberlaundering, i.e. the use of the Internet and new technologies to accomplish the cleaning of dirty money. In this regard, it is emphasized that "the offensive potential of cyberlaundering emerges, in particular, with regard to telematic transactions involving virtual currencies, on the basis of which it is possible to carry out transactions, from one part of the world to the other, at an instant speed, without barriers to entry, in total anonymity and in the absence of control by supervisory institutions".[3] The author goes on to underline how "cyberspace allows the offender to benefit, in addition to the 'dematerialization' of the resources linked to the digital content of money, the dispersion due to the difficulty of identifying the perpetrator, also of a delocalization of the user who, operating on the

[2] L. Sturzo, 'Bitcoin e riciclaggio 2.0' (2018) Diritto penale contemporaneo 19 <https://archiviodpc.dirittopenaleuomo.org/d/6006-bitcoin-e-riciclaggio-20>, 20.

[3] F. Pomes, Le valute virtuali e gli ontologici rischi di riciclaggio' (2018) Diritto penale contemporaneo 159 <http://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_pomes.pdf>, 165.

network, can be present in several IT 'spaces' at the same time".[4] An alarming observation, which, however, highlights not the criminal potential of the blockchain, but the now consolidated new scenario in which the entire economy and global finance moves, with respect to which the internet is an indispensable pillar for survival itself.

However, it is undeniable how, with respect to consolidated IT systems and electronic money, which has long found citizenship in legal economies and related sector disciplines, the spread of cryptocurrencies raises some questions about its actual danger, linked to the structure of IT protocols, and to the same philosophy that is at its origin. In particular, it was asked whether they constitute a new and more insidious risk for the legal economy or whether, they fall within the boundaries already drawn up for the criminal protection of assets and the economy, especially as regards the phenomenon of money laundering, despite the suggestions related to the characteristics of the blockchain.

3. *Bitcoins as a constituent element of money laundering crimes*

The debate on the relationship between bitcoin and money laundering crimes helps to better grasp the risks of a hasty judgment on the alleged danger of the blockchain. In fact, many scholars have highlighted how the operations carried out using bitcoins can be attributed to the constituent elements of the crimes of money laundering (648 *bis* of the Criminal Code) and self-laundering (648 *ter* of the Criminal Code), cases that are not limited to punishing the simple substitution or money laundering of illicit origin, requiring instead a *quid pluris*, that is, in the case of money laundering, that the conduct implemented is capable of hindering the identification of the criminal origin; while in self-laundering, the conduct must be further characterized by an effective, i.e. concrete, suitability to make the identification of the criminal origin more difficult. In this regard, it has been highlighted that "the probability that the Bitcoin system is transformed into a system for cleaning up international illicit proceeds will be directly proportional to the ability it will show to make it difficult to ascertain the origin of that value. Although it is undeniable that the blockchain mechanism represents a valid tool for the traceability of transactions carried out on the network via bitcoin, it is in any case demonstrated how this chain ends up coinciding with a pure mathematical matrix algorithm, not only of complex resolution, but often difficult to trace back to a well-identified natural or legal person", so that "in the case of virtual currencies, the link between the addresses of the transactions and the identity of those who actually control them is not insured". In other words, it would be anonymity to establish the essential characteristic of money laundering crimes, namely the ability to hinder the identification of the criminal origin: the pseudonym, that is the bitcoin account represented by a series of numbers and letters, which, however, once traced by the police it does not allow to go back further, in fact continuing to conceal the real physical identity of the owner of the identified account".[5]

[4] Idem, 166.

[5] Sturzo (n 2), 22.

Therefore, the obstacle does not concern the traceability of virtual money as such, but the identification of the author: this represents, however, an extensive reading of the two criminal cases, in which, instead, the criminal relevance concerns exclusively the methods of implementation of the conduct put in place by the offender. On the other hand, bitcoins are anonymous as banknotes are anonymous, the use of which may possibly constitute an indication of suspicion over their illicit origin, but certainly not a relevant conduct such as money laundering.

Conversely, it seems quite substantiated the concern of those who believe that the purchase of bitcoins with real currencies and the subsequent use of the same through a virtual wallet (so-called e-wallet), connected to the blockchain, which stores all the monetary movements attributable to each wallet, can hide an operation to clean up money of illicit origin. In this case, it would be assumed that the implementation of a replacement conduct, suitable to hinder the traceability of dirty money, which is completed with the subsequent transformation of the virtual value in one's possession into legal tender currency through the subsequent crediting of the sums of money to the current account, once converted, similarly to what happens with normal means of payment. Consider, in this regard, the presentation of a check of illicit origin at an institute of credit, with the consequent replacement of the value represented by the credit security with "clean" money, an operation deemed suitable for supplementing the money laundering conduct. Obviously, it will be necessary to ascertain, in addition to the existence of the conduct, the author's *mens rea*: an assessment that cannot be limited to a presumption, determined by the use of an operational tool – bitcoin, in fact – which has a peculiar operating complexity.

4. *Anonymity as a crime?*

Therefore, anonymity remains as an element around which the criminogenic potential of cryptocurrencies is built. This conclusion, widely shared in the doctrine,[6] does not appear entirely correct. First of all, because it doesn't seem to be true. As noted, "Bitcoins are not anonymous but pseudonyms. This means that each user is connected to a certain nickname, consisting of a long set of numerical digits that make up the address to which a particular wallet is connected. It follows that it is possible to identify the holder of the deposit, starting from the nickname use".[7] Perhaps an optimistic statement, since the pseudonym, that is the bitcoin account represented by a series of numbers and letters, once traced by the police, would not allow, however, to go back further, continuing in fact to conceal the real physical identity of the owner of the identified account.[8] More precisely, "cryptocurrencies guarantee a much higher level of anonymity than ordinary banking transactions, not only because their operating protocol does not require the identification or verification of the real identity of the holders of electronic wallets, but because [...] there are numerous tools

[6] G. P. Accinni, 'Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017' (2017) Archivio penale <http://www.archiviopenale.it/profili-di-rilevanza-penale-delle-criptovalute-(nella-riforma-della-disciplina-antiriciclaggio-del-2017)/articoli/15332>, 12.

[7] J. Sicignano, 'L'acquisto di bitcoin con denaro di provenienza illecita' (2020) Archivio penale <http://www.archiviopenale.it/lacquisto-di-bitcoin-con-denaro-di-provenienza-illecita/articoli/24907>, 13.

[8] Sturzo (n 2), 31.

that allow you to maximize the privacy of users and virtual currencies […] which are completely anonymous. The owner of an e-wallet fed with proceeds of illicit activity could therefore well dispose of it in a confidential manner, using the provision for the purchase of goods and services without leaving a trace of his actual personal details. It has also already been shown that the virtual currency system has now reached global scale, so that Bitcoin and other cryptocurrencies are easily used to make transfers at a supranational level, allowing interested parties to transfer large capital in many countries of the world. often lacking any anti-money laundering system".[9]

Therefore, this is not true anonymity, but rather a failure to identify the real user of the operation. In this regard, it could be observed that, in the world of the real economy, this circumstance occurs in a plurality of cases, all of which can be traced back to traditional forms of transactions and commercial relationships. However, the main objection, relating to the issue of anonymity, is another. The fact that the user is anonymous does not, in itself, determine the integration of money laundering conducts, at least in the forms described by the cases currently provided for in Italian law. A different conclusion can be reached in a perspective exclusively of preventive control, based on the type of perpetrator, rather than on the danger of the conduct, according to the consolidated regulatory framework that animates the entire anti-money laundering discipline, provided for by Legislative Decree No. 231 of 2007, as amended by Legislatives Decrees No. 90 of 2017 and No. 125 of 2019.[10] On the level more strictly related to criminal law, the enhancement of anonymity as a constitutive element of the conduct of re-laundering raises many doubts in relation to Art. 25 of Italian Constitution and seems to be dictated by a strong suggestion exerted by the reference to the need to combat infiltration phenomena of illicit economies in the legal fabric, as well as by the alarm raised in relation to international public order, by the continuous references to the methods of financing terrorism through cryptocurrencies.[11]

In this perspective, the hypothesis on which the alarm for the possible criminal relevance of the conduct is based is that such technologies are even conceived and developed to pursue intrinsically illegal purposes, for the sole fact of being non-compliant with established mechanisms. of exchanges and transactions and, more generally, to the general rules on the tracing of financial transactions. The context in which cryptocurrencies and the blockchain were born and have increased their consent from users is thus distorted. Their original perimeter is entirely internal to the

[9] Accinni (n 5), 20.

[10] Decreto Legislativo 25 maggio 2017, n. 90 – *Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006* <https://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg>. See C. Ingrao, 'Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio' (2019) Diritto penale contemporaneo 148 <https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_ingrao.pdf>; G. P. Accinni, 'Cybersecurity e criptovalute. Profili di rilevanza penale dopo la quinta direttiva' (2019) Sistema penale 209 <https://www.sistemapenale.it/it/articolo/cybersecurity-e-criptovalute-rilevanza-penale-dopo-quinta-direttiva>.

[11] Ibid., 149-150.

legal economy, as an expression of a cultural model that does not recognize the need for intermediation and constant control in financial transactions and operations, by credit institutions and public control agencies, in the name of a perhaps questionable and perhaps unrealistic democratization of the global economy, based, according to the approach of the supporters of such a scenario, on trust among operators, rather than on institutional control.[12]

5. *Conclusions*

The value of danger formulated with regard to bitcoins seems, therefore, strongly conditioned by a prejudice of a cultural nature, which pushes to identify the area of criminal risk regardless of the real detrimental suitability of the instrument as such. Above all, the element of anonymity is confused, which in any case affects the figure of the author, or rather his immediate identifiability, with the constitutive elements of the cases of money laundering, which do not include the intentional concealment of the perpetrator of the conduct Illicit: not all obstacle activities are punishable by way of money laundering or self-laundering, but only those that concern exclusively the reconstruction of the illicit origin of the goods or utilities that the subject intends to clean up. On the contrary, in virtual currencies, the only dissimulatory operation concerns the possible holder of the virtual currency, who would be covered by a pseudo anonymity. From a material point of view, the asset does not undergo any camouflage, resulting in perfectly traceable and visible bitcoin transactions.[13]

Therefore, if it is compatible with a criminal system centred on introducing control mechanisms in a preventive function intended to bring out the identity of the virtual user, an analogical interpretation of the types of money laundering provided for in the code system, which punishes the same only because you do not collaborate with the authority in revealing your own identity.

[12] Sturzo (n 2), 20.

[13] Sicignano (n 6), 15.

BITCOIN AND CRYPTOCURRENCIES.
TAX LAW RELATED PROFILES

GIUSEPPE RIVETTI – PAOLA CRICCO

SUMMARY: 1. Preliminary remarks. – 2. Blockchain. Data management system. – 3. Some general considerations about cryptocurrencies. – 4. Bitcoin, virtual currency. Multiplicity of meanings. – 5. Ripple, a "semi-centralized" virtual currency. – 6. Ethereum. Fast secure transactions. – 7. Fiscal regime applicable to virtual currency transactions. Tax issues. – 8. Cryptocurrencies used for illegal purposes such as money laundering and terrorist financing. Connection between money laundering and tax offences.

1. *Preliminary Remarks*

A process of growing integration of international markets and of the trade of goods, services and financial transactions entails an ever-growing number of operators whose attention turns to global perspective horizons[1]. Such internationalisation determines an opening of the different economies as a result of the increase in cross trade activities, movements of capital, new knowledge and techniques. Within the framework of such an innovative scenario it is worth remembering that in order to certify certain important activities man has always relied on the intervention of third party entities: banks in case of money transfers; notaries in case of purchase and sale of real estate or assets in general; central authorities for the validation of an indefinite list of particular operations and transactions.

By the end of the first decade of the new millennium the new technological intuition, or maybe the need to get rid of such third party entities, had inspired a person – or rather a group of software engineers whose identity is still unknown, but use the name Satoshi Nakamoto – to conceive and design a software environment system allowing the certification of certain transactions without the intervention of the above entities, persons or central authorities: a system controlled by mathematical/computer algorithms, available for everyone to cooperate to the validation of the entered information.

The purpose was the creation of a distributed software environment having the functions of a public notary, the so-called Distributed Ledger Technology (DLT). The following figure shows the infrastructural logical configuration of the DLT.

[1] In relation to the development of this occurrence, G. de la Dehesa, *Winners and losers in globalization* (Oxford 2005); G. M. Milesi-Ferretti and P. Lane, *Financial globalization and exchange rates*, (1 January 2005) IMF Working Paper N. 5/03 2005; M. Obstfeld and A. M. Taylor, *Global capital markets: integration, crisis and growth* (Cambridge 2004). J. Eatwell and L. Taylor, *Global finance at risk: the case for international regulation* (New Pr 2001); K. Okina, M. Shirakawa and S. Shiratsuka, 'Financial market globalization: present and future' (1999) 17 Monetary and Economic Studies 1; S. Strange, *Madmoney* (Manchester University Press 1998).

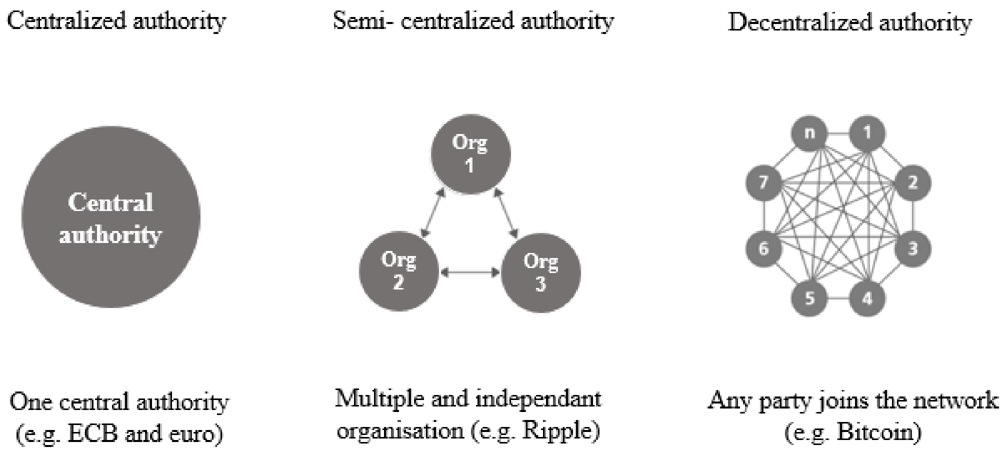

Centralized authority
Semi- centralized authority
Decentralized authority
Central authority
Org 1
Org 2
Org 3
n
1
2
3
4
5
6
7
One central authority (e.g. ECB and euro)
Multiple and independant organisation (e.g. Ripple)
Any party joins the network (e.g. Bitcoin)

Fig. 1: Structures of currencies and cryptocurrencies. Re-worked after a chart by Joshua Baron, Angela O'Mahony, David Manheim, Cynthia Dion-Shwarz, National Security Implications of Virtual Currency (Rand Corporation 2015)

Cryptocurrencies, especially bitcoins, represent an application of the above. To date there are more than 2000 virtual currencies[2] though the present paper will deal essentially with the blockchain and some of the main cryptocurrencies.

2. *Technology, ethics, and law*

The blockchain is a particular management system of information based on the above-mentioned infrastructure called Distributed Ledger Technology. The DLT is to be considered as a sort of data base whose data is not stored in a single "point" but over a number of computers or sets of computers, called nodes, connected to each other through the internet. The main characteristics[3] that have encouraged the spread of DLT environments are:

- scalability and robustness, i.e. the possibility to add or remove nodes without affecting the functional body of the network;
- open-sourcing, i.e. the software ability not only to tolerate any alteration of the source code, but above all to give the possibility to observe and evaluate the reliability of the software itself (cooperation in the correction of errors and protection from malware);
- absence of the intervention of any trusted entities or persons to certify the activities managed by the system;
- non-repudiation of the information entered in the system; and
- in relation to cryptocurrencies, "pseudo-anonymity" and traceability online of the transactions, as well as prevention of double-spending.

In short, the word "blockchain" is self-explanatory as its functioning is based on the management of a "chain of blocks": it is a digital register of transactions processed on the network in which such transactions are recorded individually in a section of the DLT called "block". On a regular basis the block is "closed", that means that in that specific section of the DLT no further transactions can be inserted nor those already

[2] These data are taken from one of the most reliable sites according to the field experts, *CoinMarketCap*.

[3] O. Calzone, 'Bitcoin e distributed ledger technology' (28 February 2017).

entered are susceptible to be modified. Such functional approach is identical for all blockchains used in the different applications, even showing some specific features with respect to different cryptocurrencies.

Each new block contains the digital signature of the previous block and the sequence of blocks constructs the chain. Such chain is visible on the network and can be freely consulted and downloaded by everyone. When modifying the data, the duration of the transaction processing can be affected in compliance with security requirements: in fact, the blockchain takes into account the whole available chronology, so that operations in DLT can be fairly slow.[4]

The "peer-to-peer" blockchain technology[5] can be applied in numerous fields.[6] In fact, it can potentially substitute for all central institutions through a distributed horizontal open network thus replacing all intermediary entities, third parties, controllers, central institutions, and having processes managed by a network of blocks that validate operations.

Bitcoin and cryptocurrency blockchains are accessible and "publicly visible", while consortium blockchains are typically "private" and accessible only by the participating institutions.[7] During the last few years, such consortia have developed their activities, especially those dealing with the financial sector, specifically interested in exploiting the blockchain technology in basically all industrial areas.

The technology represented by the blockchain in recent years has been analyzed also by the traditional institutional actors, to the purpose of analyzing all its potential applications and at the same time trying to control the implicit threat underlying such disruptive technology.

Central banks worldwide are concerned in monitoring the development of cryptocurrencies and blockchains in all their possible applications within the FinTech sector. For instance, while such new technologies started to spread, the Bank of Italy has firstly set up a dedicated multidisciplinary working group (representing all institutional, research and IT functions) in order to analyze all initiatives dealing with blockchains in the national market, verify their consistency with the current regulatory framework and identify the possible legislative gaps and relevant potential risks. In 2020 the Bank of Italy has constituted the FinTech Committee, which is nothing more than the evolution and institutionalisation of the above interdisciplinary working group, which represents the strategic pivot whose target is to encourage digitalisation in Italy (especially on the occasion of the last pandemic emergency and in view of other future

[4] It must be considered that VISA is able to process tens of thousands of transactions per second, PayPal some hundreds, while as far as virtual currencies are concerned, the bitcoin can process 7 transactions per second, Ethereum 20 and Ripple some thousands.

[5] In the peer-to-peer network, the inter-connected nodes are equal peer and function as client and server at the same time.

[6] In the last few years, many business applications have been developed exploiting the blockchain technology. Among the most popular there are those that guarantee the traceability of food; goods tracking; the completion of certifications; gaming; accounting; management of transactions, knowledge, creation of value; voting systems; legal/notary services.

[7] Public Blockchain: it is an open editable blockchain (upon consent given by the majority of the nodes), using consensus mechanisms like the proof-of-work and proof-of-stake systems. Consortium and private blockchains: the consensus can be centralized or controlled by certain nodes, and their validation and public visibility can be restricted, *La tecnologia blockchain: nuove prospettive per i mercati finanziari* (Banca d'Italia 2016).

'black swan' events), to widen the implementation of institutional offices relying on the new technologies, support families and the financial system through digital leverage, as well as to strengthen the cooperation with the other public entities on the national, European and international levels.

Taking into account the essential interrelationships existing between cryptocurrencies and the traditional banking system and, on the other hand, the potential positive effects of blockchain technology (e.g. reduction in operating costs, greater spread of information and better performance of the markets), the intention of the legislator is to encourage innovation without weakening the necessary activities of control and protection of the system, also preserving the reconciliation of the involved parties' interests.[8] With the evolution of the regulatory framework, also under the EU impetus, there will shortly be a change in the system of payments that will renew and expand this sector and its players alongside with the spread of the blockchain technology.

3. *Some general considerations about cryptocurrencies*

Within the complex changing "ecosystem" of cryptocurrencies, the bitcoin (being a pioneer in the sector) has the largest market share even though recently decreasing in its popularity by reason of the new alternative cryptocurrencies Ripple and Ethereum that are now proving a significant increase in capitalisation.

There are many other kinds of cryptocurrencies that mainly replicate the basic logic of bitcoin adapting and privileging some features over others, often depending on the pre-eminent needs of certain niches of users that have to be satisfied (e.g. speed in transactions, higher anonymity, etc.). In the following sections we will refer only to three cryptocurrencies that, to date, are among the most used: Bitcoin, Ripple and Ethereum.

The tool that allows one to complete the purchase and sale of goods, services or cryptocurrencies is called *wallet*. The main function of the wallet is to securely hold the user's private key, create transactions that are sent to the network and collect incoming and outgoing transactions, highlighting the balance available to the user. The wallet can be physical (a sort of USB stick or a simple sheet of paper showing the relevant "bitcoin address" which can be either alphanumeric and a QR code) or software (mobile application, PC program or a program on the network). The bitcoin address is the equivalent of the IBAN of the traditional banking system, so that in order to be allowed to receive bitcoins it is necessary to give a bitcoin address.

4. *Bitcoin, a virtual currency. Multiplicity of meanings*

At the beginning of 2020, the bitcoin was still the most widespread virtual currency. Born in 2008 from the theorisation of the person or persons using the pseudonym of Satoshi Nakamoto and operational since 2009, the bitcoin uses cryptographic schemes for the creation and transfer of money outside the system governed by central authorities, financial and banking intermediation and any inflationary process. In fact, it is a distributed digital currency, created from a decentralized peer-to-peer network.

[8] I. Visco, 'La tecnologia blockchain: nuove prospettive per i mercati finanziari', in *La tecnologia blockchain: nuove prospettive per i mercati finanziari* (Banca d'Italia 2016).

Nonetheless, the word "bitcoin" has several meanings as specified hereunder:

- The protocol: these are instructions on how to build the blockchain, how it is to be analyzed, how to assemble transactions and features that make a transaction valid;
- The network: it is the peer-to-peer network that connects the nodes whose function is to carry messages managed by the protocol;
- The currency: bitcoin is normally written with the lowercase initial and is the original unit of the Bitcoin network, constituted by 21 million bitcoins in circulation. The bitcoin is the main unit of measurement, and each one is divisible into 100,000,000 parts called "satoshi".[9]
- The open-source implementation: it is the original open-source project, written in computer language, which implements the protocol. From the website <bitcoin.org/en/download it> is possible to obtain the source code freely and without cost.

The bitcoin network is managed peer-to-peer directly by its users, who contribute to the smooth operation in a decentralized manner for the "certification/closing" activities of the blocks. The algorithm that is at the base of the bitcoin software allows the creation of only 21 billion bitcoins. It is estimated that there are about 18.4 million units in circulation for a total value of approximately 160 billion dollars.

Bitcoins are created through the so called "bitcoin mining" that consists in the resolution of complex calculations, sometimes sharing the computing power of many computers in "bitcoin farms" or by "cloud mining", i.e. renting computing power; such use of resources is remunerated by the issuance of some units of cryptocurrency whose amount, initially fixed in 50 bitcoins, is halved every four years approximately, in parallel with the decreasing amount of the virtual currency issued. People or entities that perform bitcoin mining are commonly called "miners"; their function is essential for a new block of transactions to be added to the blockchain and for the control, validation, and encryption operations to be completed.

Generally, crypto value networks reward the calculation of the correct hash with a predetermined amount of currency, which is also an incentive for the users who make their computing power available for transaction security. Since there is no centralized entity responsible for the remuneration of certification activities, it is the system itself that provides for the remuneration of those who handle the blockchain management operations. This function allows for each closed block a certain number of bitcoins to be given to the entity that closes the block. The management protocol of the closing of the block provides for the halving of the bitcoin reward value every 210,000 blocks. Under the operating rules of the bitcoin blockchain, this condition occurs about every 4 years. The last one was on 12 May 2020.

[9] C. Richard, *Learning bitcoin* (Packt Publishing 2015), 9.

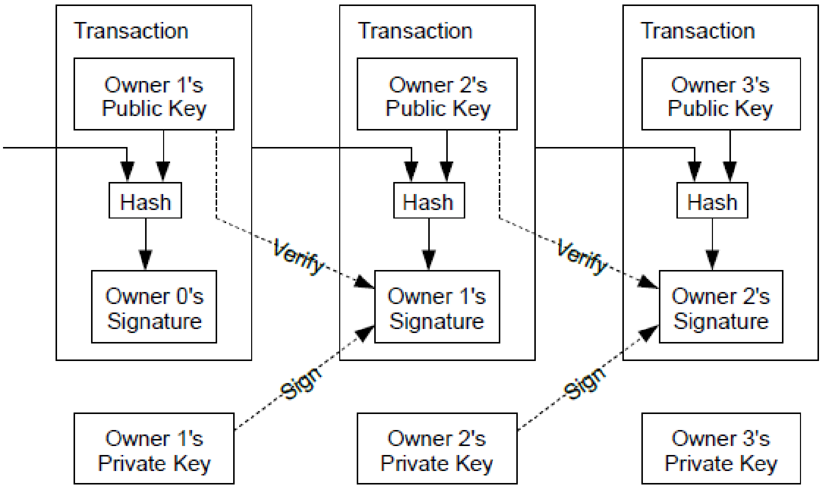


Fig. 2: Bitcoin transactions – Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008)

The bitcoin is based on a distributed consensus algorithm using the proof-of-work mechanism (PoW). An alternative way to validate transactions is to allow nodes to hold a certain amount of money for a certain time (coinage) to be used as collateral for the transaction eventually certified; this is the proof-of-stake that does not require complex calculations (likewise for the bitcoin) to validate transactions in the ledger. Such mechanism is used by Ripple, that has become recently the second most used cryptocurrency after the bitcoin, whose blockchain is the basis of a payment system.

In Italy, in a context particularly prone to the use of cash, cryptocurrencies are still moderately popular, even if it must be said that they are more and more frequently used in different commercial sectors, such as clothing, restaurants, in the e-commerce, and even cab services and real estate business.

Nevertheless, the strong growth of the use of bitcoins (BTC), which was not expected nor predictable, has highlighted some critical points, in particular the limits shown by the decentralized certification chain of transactions and the limits of the capacity of the blocks (one megabyte per block). With the substantial increase in the number of transactions, such characteristics have entailed longer delays in the processing of these transactions and higher commissions: these are elements that slow down the spread use of bitcoins.

5. *Ripple, a "semi-centralized" virtual currency*

Ripple (XRP) was created in 2012 and has now become one of the main cryptocurrencies after bitcoin. Ripple's characteristic, as shown in Figure 1[10] is being "semi-centralized" with respect to the presence of a central authority (not necessarily public), because it is connected to a network in which there are some nodes that act as validators, in other words certify transactions, and at the same time guarantee efficiency and short delays of processing. Ripple's blockchain has been conceived with the aim of making intercontinental payments fast, eliminating a series of intermediaries and delays

[10] J. Baron, A. O'Mahony, D. Manheim and C. Dion-Shwarz, *National Security Implications of Virtual Currency* (Rand Corporation 2015), 9.

typical of the traditional systems, and its technological infrastructure currently allows different types of assets to be exchanged.

The method of validation of the distributed ledger is certified by major telecommunication companies and by academic bodies (including the Massachusetts Institute of Technology). This has awoken the interest of many credit and financial institutions in a considerable way. In order to guarantee the consistency of the data of currency movements banks, or authorities must set up an adequate security system, involving some costs: the adoption of the Distributed Ledger Technology simplifies these activities and enhances their effectiveness. Ripple can rely on an increasing support from traditional credit institutions, since many banks and international financial institutions belong to RippleNet, a global decentralized network of banks and payment institutions using the blockchain bearing the same name[11]. The banking circuit that has adopted Ripple is at present evaluating the possibility of using the infrastructure also for the management of a new payment card system.

6. *Ethereum. Fast and secure transactions*

Ethereum was developed in 2014, its security features are more accurate if compared to those of bitcoins and has a peer-to-peer sharing structure where information is managed on multiple nodes at the same time making it more complicated for hackers to penetrate and modify data.

Ethereum's blockchain is very successful thanks to its optimal trade-off between security and speed of the transaction process and has become the reference platform for several start-ups, well beyond the mere cryptocurrency payment processing industry,[12] in particular for the potential offered by smart contracts whose conception is not new but largely extending to different fields since the development of blockchain technologies.

The main features of the Ethereum environment allow cryptocurrencies to be used not only in case of traditional transfers of virtual currency. Two further particular activities can be processed:

a) Fundraising: ICO (Initial Coin Offer) is a mechanism according to which a company, in order to finance its projects, relies on certain Ether lenders whose intervention is both an investment and a sort of “fidelity card” through which the lenders can receive the benefits generated by the company that launched the ICO
b) Smart contracts: the so-called "smart contracts” use the Ethereum underlying logic in order to implement software procedures that manage the relationships between users, taking into account a whole series of parameters that characterize a contract, i.e. negotiation, execution, partial or total exclusion of a contractual clause. All this without the need of the intervention of a public notary to formalize the system operation. There are two types of smart contract:

[11] ABI, *Banche italiane avviano sperimentazione blockchain* (4 June 2018).

[12] Among others, applications like uPort, whose object is to replace the identity cards issued by the state authority with a certified digital identity, and GridPlus, used to track power consumption to the purpose of cutting the cost of energy bills.

- Smart Code Contract: it has no legal value, and its use is limited to the management of each status of a process to be controlled. Each status is a transaction of the process, and all the transactions are stored in the blocks.
- Smart Legal Contract: it has a purely legal content. When certain conditions of the process under analysis occur, the system starts certain particular actions.

7. *Fiscal regime applicable to virtual currency transactions*

Possession of bitcoins and cryptocurrencies must be declared to the tax authorities by entering the information in section RW of the tax return. In fact, by judgment No. 1077 of 27 January 2020,[13] the Regional Administrative Tribunal (TAR) of Lazio rejected the appeal lodged by the concerned associations[14] challenging the decision according to which "virtual currencies" are to be subjected to the fulfilment of the obligations in relation to the so-called tax monitoring referred to in Law Decree No. 167 of 28 June 1990. The fulfilment of such obligation is in fact imposed by the Inland Revenue through the publication of the guidelines for the compilation of the 2019 tax return form for natural persons although in the absence of any act providing for this obligation.[15]

[13] See Regional Administrative Tribunal (TAR) Lazio (Sect. II – 3), judgment No. 1077 of 19 November 2019 – 27 January 2020. The judgment stems from the appeal brought by some associations against the 2019 income declaration forms (tax year 2018) which provided for the inclusion of virtual currencies within the tax monitoring obligations.

[14] These associations (as for example ASSOBIT) spare no efforts to promote the widest spread of the Blockchain technology and represent the interests and instances of all those who carry out activities related or attributable to it (such as, for example, the development, production, distribution, marketing of related software and hardware, relevant services such as trust deposits, management of wallets, exchange or purchase and sale of cryptocurrency, etc.).The above associations challenge the judgment for the following reasons. Nullity ex Art. 21-septies of Law No. 241/1990 of the contested measure for absolute lack of authority by the Administration to provide for the introduction of the described tax regime to "virtual currencies" according to the provisions of Art. 23 of the Constitution and Art. 1 of Law No. 212 of 27 July 2000 (the subjection of virtual currencies to tax declaration obligations referred to in the contested measures would be the result of the exercise of an administrative power without any primary rank legislative authority). Infringement and/or misapplication of Art. 1 of Presidential Decree No. 322 of 22 July 1998 – Breach of law - of Articles 5 and 7 of Law No. 212 of 27 July 2000 (the so-called Charter of Taxpayer Rights) and misuse of powers for failure to state reasons, misrepresentation of facts and lack of proper preliminary investigation (lack of a formal measure of approval or modification of the tax return model; violation of the taxpayer's right to be duly informed). Infringement and / or misapplication of Articles 1 and 4 of Law Decree No. 167 of 28 June 1990 (so-called decree on "tax monitoring"), Art. 9 of Law Decree No. 917 of 22 December 1986 (so-called "T.U.I.R." – *Consolidated Law on Income Tax* – [*Translator's note]*) and Art. 1, paras. 2, 3 and 5, of Law Decree No. 231 of 21 November 2007 (so-called "Consolidated Law Anti-Money Laundering"), as amended by Law Decree No. 90 of 25 May 2017 (transposing Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, so-called "Fourth AML Directive"). Annulment of the contested measures because contrary to European law, subject, if necessary, to a preliminary ruling as provided by Art. 267 TFEU.

[15] The applicant associations assume that the virtual currencies, first among all the bitcoins, are digital recordings stocked in ledgers ("blockchains") whose distributed and shared copies remain in all computers or devices connected to the network they belong to; moreover, virtual currencies are nothing less than empty virtual boxes eventually available to be filled with data and transmitted to other users. Furthermore, virtual currencies have been positively recognized by Italian Law thanks to Law Decree No. 90 of 25 May 2017; in the transposition of the Fourth AML Directive (Directive (EU) 2015/849),

In addition, the applicant associations maintain that the measures they challenge are illegitimate also on the ground of the illogicality and unreasonableness of the operated assimilation, for tax purposes, of virtual currencies to foreign investments and financial activities[16]. In this regard, the above associations represent a series of motivations: (i) virtual currencies are not included in the typical list of incomes referred to in Art. 6 of the T.U.I.R., (ii) the mode of preservation is not referable to a "geographical" concept of possession[17] and, finally, (iii) the providers of the services concerning the use of virtual currency are not comparable to financial operators.[18]

However, the judges[19] note that the Inland Revenue by Interpellation No. 956-39 of 2018[20] had already expressed the concept that possession of virtual currencies must be declared. Therefore, the instructions take over and formalize a pre-existing orientation.[21] In any case, it appears conclusive the regulatory amendment to Law Decree No. 167/1990, made through Law Decree No. 90/2017 (with regard to the fight against money laundering) which has explicitly included the use of "virtual currencies" among the relevant operations to be subjected to monitoring.[22]

Also from this further point of view, therefore, it is confirmed that these "instructions" are not an innovation of the tax system, but rather a sign of the change in the monitoring regime implemented as a result of Law Decree No. 90/2017.[23]

the legislator has introduced a definition of "virtual currency" recalling the one contained in the Commission's proposed amendment, thus anticipating the transposition of Directive (EU) 2018/843 (so-called Fifth Anti Money Laundering Directive) dated 30 May 2018.

[16] In this connection, please refer to «*Virtual currency schemes – a further analysis*» (2015) a report by ECB in which it is established that for regulatory purposes virtual currencies do not fit the legal definition of tender currencies, being no creditor obliged to accept payment in virtual currency to discharge a debtor of its debt. Furthermore, the European Court of Justice, by a judgment dated 22 October 2015 (case C-264/14) in relation to a case of intermediation carried out through exchange transactions between virtual and legal tender currencies, established their non-validity with respect to VAT purposes.

[17] The blockchain as such is a shared distributed "virtual ledger" that keeps track of all messages received by every individual user of the system. Its essential feature is therefore its "aterritoriality" since the availability of the virtual currencies coincides with the possession of a "private key", essential for their transfer (which key, in turn, is a unique "cryptographic code") which cannot be considered as a "storage" in a physical place.

[18] See Art. 3, para. 5, of Law Decree No. 231/2007 (modified by Art.1 of Law Decree No. 90/2017).

[19] The judges maintain that the action of the applicant associations aiming at the annulment of the contested measures by which the Inland Revenue has subjected the "cryptocurrencies" or digital currencies to administrative taxation is legally groundless, also due to the impossibility to assimilate the character and the nature of such currencies to income of financial nature. In particular, it is exactly for this reason that they are not included in the list of Art. 6 of the T.U.I.R. (Presidential Decree 917/1986).

[20] See Interpellation No. 956-39 of 2018. This orientation corresponded to what was perceived by legal theory (and more precisely in the comments to the 2018 tax obligations relevant to 2017).

[21] Ibid.

[22] Basically, the regulatory innovation expressly submits to monitoring the use of virtual currencies and establishes that both financial and non-financial operators are subject to the same monitoring.

[23] The judges point out that it is a matter of specific regulatory interventions aimed at giving a formal classification to the categories of transactions performed using virtual currency, helping to define the relevant applicable regime especially for the purposes of monitoring and for the prevention of money laundering, but with obvious repercussions also in terms of tax liability. In fact, such classification is not limited to define virtual currencies money as a "means of exchange", but expressly contemplates the possibility that through its use a number of operations of "purchase of goods and services" or "investments" can be completed, transposing that ductile characteristic of the "digital representations of values" – which allows to convey more types of operations and exchanges. Moreover, from the point of

After all, the admittance of the notion of "functionality" of virtual currency involves its liability to taxation not because it is a financial means in itself, but because of the different purposes that the use of virtual currency makes possible (financial purposes or purchase of goods and services, as the case may be). As a consequence, the guidelines of the Inland Revenue expressed in Resolution No. 72/E of 2 September 2016[24] and in the Interpellation No. 956-39/2018 are not inconsistent with the "instructions" object of the annulment action in question.

With reference to the tax treatment strictly applicable to transactions linked to virtual currencies, as specified by the Inland Revenue with the aforementioned Resolution No. 72/2016, we cannot ignore what the Court of Justice of the EU stated in its judgment of 22 October 2015, Case C-264/14. In particular, it is thereby clarified that the activity of intermediation of traditional currencies with bitcoin carried out professionally and on a regular basis involves VAT as well as IRES (*Corporate Income tax*) and IRAP (*Regional Income Tax)* liabilities.[25]

On the contrary, in the case that natural persons hold bitcoins (or other virtual currencies) outside their business activity, the general principles regulating operations with traditional currencies are applied. As a consequence, movements of virtual currency do not give rise to taxable income in the absence of speculative purposes, unless a different income is generated because the transferred currency derives from withdrawals from wallets (electronic portfolios), whose average stock exceeds a

view of the legislation, Law Decree No. 90/2017 and Directive (EU) 2018/843 of 30 May 2018 have completed the scenario. Such Law Decree and Directive include a formal definition of virtual currency as a "means of exchange" (Art. 1, para. 2, let. q) of Law Decree No. 231/2007, as amended by Art. 1 of Law Decree No. 90/2017).

Moreover, in the final wording after the amendments made in the course of the case to Article 1 of Law Decree No. 231/2007 by Law Decree No. 125 of 4 October 2019 (therefore subsequent to the contested measure, but still relevant to guide the interpreter), "virtual currency" is "the digital representation of value, not issued or guaranteed by a central bank or public authority, not necessarily linked to a legal tender currency, used as a means of exchange for the purchase of goods and services or for investment purposes and transferred, stored and traded electronically".

Under subparagraph (s), the words "means of payment" define the following: "[…] every other available instrument that allows to transfer, move or acquire, also electronically, funds, values or financial resources"; finally, at subparagraph (ff) the "providers of services related to the use of virtual currency" are "every natural or legal person that supplies to third parties professional services functional to the use, exchange, custody of virtual currencies and their conversion from or into currencies having legal tender".

[24] We recall the principles expressed by the Court of Justice of the EU (Case C-264/14, *Skatteverket v David Hedqvist*, judgment of 22 October 2015) that, in relation to indirect taxes (VAT), specified that "transactions consisting in the exchange of traditional currency against units of virtual bitcoin currency [...] constitute services for consideration". Therefore, taking into account Art. 135, para. 1, let. a), of Directive 2006/112/EC, it is "clear that the bitcoin has no other purpose but that of a means of payment, and it is accepted for that purpose by some operators". Therefore, these operations, as far as VAT is concerned, are to be qualified as exempt (Art. 10, para. 1, no. 3, Presidential Decree No. 633/72). For the purposes of direct taxation, the Inland Revenue considers that the taxpayer "must declare the income deriving from the intermediation activity of purchase and sale of bitcoins, net of the related costs inherent to this activity".

[25] Subject to the obligations of adequate customer verification, as well as registration and reporting requirements provided for by Law Decree No. 231 of 21 November 2007.

countervalue of EUR 51,645.69 for at least seven consecutive working days in the tax period.[26]

In other words, the Inland Revenue has specified that the bitcoin is similar to any currency and therefore the same regulations apply to private individuals who engage in speculative activity in the monetary field. This regulation establishes that only the activities of private citizens who hold for at least seven consecutive days in a year an amount in currency for a countervalue equal to or exceeding EUR 51,000 can be considered speculative activity (thus generating taxable income).[27]

8. *Cryptocurrencies used for illegal purposes such as money laundering and terrorist financing. Connections between money laundering and tax offences*

As a different approach, the G20 member countries (20 March 2018) refuse to consider bitcoins and other cryptocurrencies as national sovereign currencies. Moreover, they are aware of the risk that such cryptocurrencies may be used for illegal purposes, such as money laundering and terrorist financing,[28] just because of their "crypto" nature. The elimination of anonymity, characteristic that may encourage illegal behaviours, could be a first attempt to solve the highlighted problems.

The management of cryptocurrency is still the object of different views invoking stricter or lighter regulations of the sector. It is therefore necessary, in this general context in which the States have not yet found a unified position, to implement a new regulatory framework.

On the other hand, the growing globalisation of finance opens the way to criminal behaviours, generally identifiable mainly in money laundering.[29] In this perspective, the effects are not reflected only in the economic sphere, since such illegal operations risk to affect negatively also factors of growth and social development of the States.[30] It is

[26] Pursuant to Art. 67, para. 1, let. c-*ter*) of T.U.I.R. In this context, in consideration of the fact that in the previous petitions the taxpayer had merely asked whether the spot transactions were subject to taxation but omitted to give any indication of the real average stock of all its wallets, in addition to what specified by the Inland Revenue in its replies to the previous petitions it is clarified that should such stock have exceeded the countervalue in Eur of 51.645.69 for at least seven continuous working days in the tax year 2016, also the exchange transactions carried out in that tax period would be subject to taxation in compliance with the combined provisions of Art. 67, para. 1, let. c-*ter*), and para. 1-*ter*, of the Consolidated Law on Income Taxes approved by Presidential Decree No. 917 of 22 December 1986.

[27] In this case the capital gain must be recorded and declared. However, private investors do not "file their balance sheet" at the end of the year, so the capital gains (26% of the gains or capital gain) will be recognized only at the time when the bitcoins shall be sold.

[28] See, *inter alia*, the qualification of international terrorism introduced by Law Decree No. 144 of 27 July 2005, providing for urgent measures to combat international terrorism (converted into Law No. 155 of 31 July 2005).

29 In this context of globalisation of the economy, the provision of valid and effective international control bodies is therefore fundamental, together with adequate prevention and contrast instruments. In fact, it is often a matter of financial flows from criminal activities introduced into the legal economy in order to conceal their illegal origin.

With reference to the distorting effects of money laundering on market mechanisms, see, World Bank, Governance, the World Bank's experience, Washington, 1994; UNDP (United Nations Development Programme), *Human development report,* Washington, 1991.

[30] In this regard, see Bank of Italy, *Comunicazione UIF del 23 aprile 2012 – Schemi rappresentativi di comportamenti anomali ai sensi dell'art. 6, co.7, lett. b) del d.lgs. No.231/2007. Operatività connessa con le frodi fiscali internazionali e con le frodi nelle fatturazioni* <https://uif.bancaditalia.it/normativa/norm-

no coincidence that criminal practices[31] determine a drop in general economic levels, and financial instability can lead to the progressive impoverishment of entire segments of the population, especially in those weaker systems that have placed excessive reliance on international finance.[32]

In this context, the relationship between money laundering and tax crimes is the core subject-matter of an intense debate of legal theory, also following recent innovative case-law material. In this regard, the judges of the merits on the ground of previous case-law were inclined to exclude the possibility to represent a relation existing between money laundering and tax crimes. Indeed, it was maintained that tax fraud could not constitute a valid prerequisite condition to money laundering activities, due to the concrete impossibility of identifying the nature and size of the illicit proceeds.[33] Therefore, it was affirmed the principle according to which the assumed offence of money laundering could "only consist of crimes that produce an evident and tangible enrichment of the perpetrator of the crime. An enrichment that must be physically locatable" and therefore, "isolable [...] and recognizable within the assets of the author of the unlawful behavior", referring, in this regard, to the "identifiability" of the proceeds "as interpreted by civil law".

However, following the implementation of the aforementioned Directives of 2001 and 2005 – with consequent extension of the number of the predicate offences – and the FATF's Forty Recommendations (February 2012), the crime of money laundering has been included within the serious offences, including tax offences. The same Directive (EU) 2015/849 expressly identifies all tax offences concerning direct and indirect taxes among the criminal activities "relevant" to money laundering.

Therefore, in view of the changed EU and international contexts, the national legislator has taken steps to revise the regulatory framework on the subject, highlighting the systematic connection between money laundering, self-laundering[34] and tax offences.

indicatori-anomalia/COMUNICAZIONE_UIF_DEL_23_Aprile_2012.pdf>. Following the update of the anomaly indexes, it should be noted that there is a close relationship between tax evasion and money laundering; low tax countries are the most subjected to such unlawful behaviours.

[31] See U.S. Presidential Commission on Organized Crime, *The Cash Connection: Organized Crime, Financial Institutions and Money Laundering* (1984) and taken up in legal theory from: D. Masciandaro and A. Mantica, 'Evoluzione del sistema pagamenti internet e cybericiclaggio: prime riflessioni', in F. Bruni and D. Masciandaro (eds), *Mercati fiduciari e riciclaggio. L'Italia nello scenario internazionale* (EGEA 1998), 57 ff.

[32] See also Senato della Repubblica, *Problematiche connesse al riciclaggio nell'ambito dei disegni di Legge n. 733 e collegati in materia di sicurezza pubblica.* Testimonianza del Governatore della Banca d'Italia Mario Draghi (15 July 2008). With negative consequences on the reputation of the financial institutions in terms of adherence to standards of honesty and compliance with standards and ethical codes by operators, M. Draghi, *L'azione di prevenzione e contrasto del riciclaggio* (Banca d'Italia 2007).

[33] Legal theory, L. Tosi and A. Toppan, *Lineamenti di diritto penale dell'impresa* (CEDAM 2017); E. Della Valle, 'Le operazioni inesistenti nell'ordinamento penal-tributario' (2015) Rassegna tributaria 433; S. Giavazzi, 'I reati societari e fiscali quali reati-presupposto del riciclaggio', in S. Giavazzi and M. Arnone (eds), *Riciclaggio e imprese. Il contrasto alla circolazione dei proventi illeciti* (Vita e Pensiero 2011), 108 ff; P. Ielo, 'Reati tributari e riciclaggio: spunti di riflessione alla luce del decreto sullo scudo fiscale' (2010) Rivista 231 10; F. Hinna Danesi, 'Proventi da frode fiscale e riciclaggio', in C. G. Corvese and V. Santoro (eds), *Il riciclaggio del denaro nella legislazione civile e penale* (Giuffrè 1996), 283 ff. See, also, G. Flora, 'Sulla configurabilità del riciclaggio di proventi da frode fiscale' (1999) Foro Ambrosiano 44.

[34] See A. Gullo, 'Autoriciclaggio e reati tributari' (2018) Diritto Penale Contemporaneo <https://archiviodpc.dirittopenaleuomo.org>; L. Deaglio, 'Autoriciclaggio e reati tributari: lo scontro

As it is formulated at present, Art. 648 bis of the Italian Criminal Code does not contain the previous mandatory specification regarding the predicate offences, but its object has been developed so as to include also the "substitution or transfer of money, goods or other benefits" and all behaviors that may hinder the identification of their criminal origin.

By adding the specification "other benefits" as a last provision in relation to "money and goods", the rule aims to prevent that such benefits generating unlawful profit may "elude" criminal repression.[35]

On the other hand, the wording "other benefits" is so broad that it includes everything that has an economically appreciable value, such as the *res* that automatically increase the assets of the wrongdoer, or any type of fraudulent activity aimed at preventing the impoverishment of assets.[36]

As highlighted by the recent case-law, the historical evolution of the rule and its literal wording[37] leads to believe that all fraudulent crimes (and, therefore, also tax frauds) are included among the predicate offences. In this regard, it is necessary to consider how tax frauds[38] (including those carried out at international level) and money laundering are functionally linked crimes. In many instances, in fact, tax evasion represents the instrument used to constitute funds to be reinserted into the economic circuit or to facilitate criminal conducts.[39]

dottrinale in punto di compatibilità', in A. Rossi and S. Quattrocolo (eds), *Autoriclaggio. La sistematica punitiva* (Editoriale Scientifica 2017), 103; P. R. Cordeiro Guerra, 'Reati fiscali e autoriciclaggio' 2016 Rassegna tributaria 321; M. Maugeri, 'L'autoriciclaggio dei proventi dei delitti tributari', in E. Mezzetti and P. Piva (ed.), *Punire l'autoriciclaggio: come, quando e perché*, (Giappichelli 2016), 102 ff.

[35] See Art. 3, para. 4, let. f), Directive (EU) 2015/849, 20 May 2015. See also Art. 3, para. 1, Law No. 186/2014 that has also introduced the crime of self-laundering in our system.

[36] See Court of Cassation (Criminal Section II), judgment of 15 February 2012, No. 6061, and judgment of 30 January 2018, No. 11836. For the purpose of the identification of the crime of money laundering, the Judges of the Supreme Court of Cassation deem that it is of essence only "to reach the logical proof of the illegal origin of the benefits of the transactions carried out".

[37] On the issue, the decision of the Court of Cassation No. 6061/2012 (n 37), according to which the wording "other benefit" is so broad that it must include all those benefits that have an "economically appreciable value", with the consequence of including "not only those elements that increase the assets of the actor but also everything that is the result of those fraudulent activities thanks to which it is possible to prevent the assets from suffering from impoverishment", see Court of Cassation No. 6061/2012 (n 37); in accordance with Court of Cassation (Criminal Section II), judgment of 11 November 2014, No. 47436. See also Court of Cassation (Criminal Section II), judgment of 18 April 2018, No. 17235.

[38] F. D'Arcangelo, Frode fiscale e riciclaggio' (2011) Rivista dei dottori commercialisti 334; I. Caraccioli, 'Il riciclaggio di denaro proveniente da frode fiscale' <www.odcec.torino.it/public/elaborati/to21.doc>.

[39] In this regard, see Bank of Italy, *Comunicazione UIF del 23 aprile 2012* (n 31), in compliance with Art. 6, para. 7, let. b) of Law Decree No. 231/2007 – *Operations connected with international tax fraud and billing fraud*, 23 April 2012. Following the update of the anomaly indexes, it is to be noted that there is a close relationship between tax evasion and money laundering; the main vehicle is represented by low-tax countries.

BLOCKCHAIN AND ICOS (A SISYPHEAN JURIDICAL TALE ON FINANCIAL MARKETS AND INNOVATION)

ALDO LAUDONIO

> "Aye, and I saw Sisyphus in violent torment, seeking to raise a monstrous stone with both his hands. Verily he would brace himself with hands and feet, and thrust the stone toward the crest of a hill, but as he was about to heave it over the top, the weight would turn it back, and then down again to the plain would come rolling the ruthless stone. But he would strain again and thrust it back, and the sweat flowed down from his limbs and dust rose up from his head". (Odyssey, XI, 593-600)

SUMMARY: 1. Introduction. – 2. Short description of the phenomenon. – 3. Security tokens between company and financial market laws. – 4. Over the wall, chasing Sisyphus.

1. *Introduction*

Since the dawn of time the building of walls has accompanied the development of mankind and with their two sides, they have always served a dual function, to protect from the outside and to circumscribe the interior, sometimes segregating it.

Intangible walls have also been erected over the centuries, yet more than perceptible in their existence, and, among these, juridical ones are some of the richest in terms of implications for human evolution: It is not without reason that the presence of a set of rules is one of the most relevant parameters for the recognition of identity and the level of civilization of a community, which, furthermore, strengthens its social bond.

By means of simplification, it can be said that one of the fundamental aspects of legal experience is precisely that of its own delimitation – the definition of its own boundaries: the choice to regulate an aspect of the real inevitably draws a distinction between what is legally relevant and what is not, this in turn separates the typical from the atypical and the compliant from the non-compliant. This observation is linked to another that sees the legal phenomenon as a logical appendix and with delayed (and fragmentary) maturation in comparison to reality: the increasing complexity of the latter has pitilessly highlighted the multiple profiles of inadequacy of law, which from "general", "abstract", "certain", "organic", "terrible" has become "singular", "contingent", "mild", "soft", "liquid", "fluid" and, even (since not recently), "contingent".

Continuing within the metaphor of debut, we have passed from the enormous and articulated legal strongholds represented by the codes, the result of Enlightenment thought and positivism of the nineteenth century, to a series of increasingly scattered and precarious forts, outposts and trenches that, isolated and subject of constant reconstruction, guard an increasingly less recognizable frontier, far removed from the core of principles and values of each legal system.

The (un)recognizability limits of law – or, in any case, the growing problem of its identification with respect to the ragged no man's land immediately close – intertwines inseparably with the "inexpressiveness" of the sets of rules designed to govern increasingly circumscribed and specialized sectors of social and economic experiences. "Inexpressiveness" to be understood as an impossibility or, in any case, a substantial difficulty in identifying the axiological basis of the choices underlying the regulatory framework and understanding its rationale.

These initial hints allow us to approach one of these frail outposts of the juridical experience where the tension between the constant evolution of economic activities and the regulatory fabric developed to regulate them is acute and tangible: we refer to financial markets law. Within this context, almost all the main symptoms of the inadequacy of the law with respect to the phenomena destined to be subject to its domination are transparently revealed.

The cyclical succession of crises partly attributable to the unfit regulatory response and the subsequent "corrective" interventions, besides pointing out the fragmented nature of a sectoral system that goes from the plethora to the gap, highlights the presence of constant – and not always commendable – centrifugal tendencies with respect to regulatory burdens. The observation of the vast array of changes, rethinking, additions and removals to the legal texts gives the impression of a perpetual, disarranged pursuit of market players: the tension towards completion (which should be supported by a systematic project yet lacking) is constantly frustrated by new advances that bring the regulatory "boulder" downstream as soon as it was believed that it had finally been placed on top.

This inexhaustible dispute between fugitives from the legal "walls" of the financial markets and the proponents of their expansion is today witness to a new episode, apparently localized, but in reality susceptible to have very wide repercussions on the province of the law referred to: we are talking about the advent of *Blockchain*[1] technology and its reflection on the implementation of financing operations for the benefit of small businesses, conventionally defined as Initial Coin Offerings (ICOs), with an acronym carefully crafted on the established – and regulated – Initial Public Offerings (IPOs), so as to set an evocative relation.

The following pages will start with a brief overview on the multiform dynamics of these transactions, then some of the main problems that they pose between company law and financial markets law will be studied and, finally, an opinion will be drawn on the legislative choices made in the face of innovative phenomena and their fundamental inadequacies.

2. *Short description of the phenomenon*

[1] The reader should be advised that although the term Blockchain has essentially become its eponymous designation because of its notoriety, actually represents a type of Distributed Ledger Technology (DLT) as it distinguishes only one of the protocols through which a DLT can be structured (see European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), P8_TA(2018)0373): Blockchain in particular is the one associated with the issuance and exchange of the virtual currency Bitcoin. Also, it is rare that a brand new protocol is specifically created for the realization of an ICO, while, on the other hand, it is often employed, with appropriate adaptations, a protocol already set up for the creation and the operation of already established DLTs (such as, for example, the *Ethereum* ERC 20 protocol).

If, as is inherent in its nature, the law lags in the wake of technological evolution and still finds it difficult to form sufficiently elastic definitions to be superposed on reality and receive widespread adherence, a first conventional approximation may be attempted for the purpose of the following discourse.

Common to the various ICOs is the circumstance that there is an entity that issues tokens in order to collect financial resources to be allocated to an entrepreneurial project (frequently digital and online) and at the same time one can observe the lack of the penetrating professional intermediation activity otherwise imposed on the IPOs, on which the current model of regulation of financial markets is based.

The minimum representative unit of the investment in an ICO, the token, is in fact a label, which in its bare simplicity proves to be completely neutral, since entirely heterogeneous purposes can be fulfilled by using such instruments. The key to the growing success of tokens and of the disintermediating ambition at the root of a large part of the Fintech phenomena does not lie, however, on their intrinsic difference to the variety of similar, known and regulated means of raising capital, but on an extrinsic variant, shaped by Distributed Ledger Technology (DLT), about which a brief digression is imposed.

This technology is based on the telematic sharing of a digital register (or, more generically, database) distributed on multiple interconnected nodes: the operation of this register is governed by consent algorithms and smart contracts,[2] i.e. programs that, run on the nodes of that register, replicate the instructions given in the form of a source code and allow them to be executed. The result is the creation of an environment in which the same register is kept and constantly updated automatically by each node that composes it.[3] Various configurations of this environment can then be distinguished because of the greater or lesser freedom with which one can access it and make changes to the register: permissionless DLT and permissioned DLT, therefore, will be placed at the two ends of the spectrum, depending on whether there is not or vice versa it is required an authorization to be admitted and have the right to alter the contents of the register. It should be remembered, however, that the alternative is not exclusively binary and that there may be many additional intermediate modes suitable to variably accomodate in the hands of one or more users the possibility of admitting new participants or even to determine changes in the shared register.

Thanks to the creation of such a widespread telematic infrastructure, the very same tokens come into existence, formed by alphanumeric codes accessible through cryptographic keys, that bind them exclusively to their respective owners and convey the rights attributed to them. Thus, the conditions for the constant identifiability of the holder of each token are pre-established, as well as the transferability of the latter (with

[2] Under Italian law, a smart contract consists of "a computer program that operates on technologies based on distributed ledgers and whose execution automatically binds two or more parties on the basis of the effects predefined by them" (Art. 8-*ter*, para. 2, first period, Law Decree No. 135/2018).

[3] The same normative text cited in the previous note also refers to a definition of "technologies based on distributed ledgers", which are identified as "computer technologies and protocols that use a shared, distributed, replicable ledger, simultaneously accessible, architecturally decentralised on a cryptographic basis, allowing the recording, validation, updating and storage of data, both clear and furtherly protected by encryption verifiable by each participant, unchangeable and unmodifiable" (Art. 8-*ter*, para. 1, Law Decree No. 135/2018).

the associated realisation of a precondition for their negotiability[4]), its traceability in the secondary market and the tendential certainty and irreversibility of transactions, preventing phenomena of over-emission or over-circulation.

As is evident, these aspects intercept conceptually, overwhelming them, the pillars on which rests a large part of the regulatory architecture of financial markets (suffice it to think of the frontal contrast with the compulsory intermediation in the trading on the markets, with the concentration of transactions on regulated markets in principle restored with MiFID2, with the centralised management of financial instruments, with the role of central counterparties in the clearing and settlement of market transactions…): although the DLTs need further development in order for them to aspire to replace the complex grid of infrastructures and qualified agents in place – which is partly conditioned by the level of technological advancement, partly imposed by the sheer complexity of the legislation – both national and supranational authorities and many economic operators are exploring their specific risk profiles, as well as the functional equivalence margins with respect to centralised registers and other centralisation phenomena that can be found in the functioning of markets.

In all this, tokens – technically and also etymologically "symbols" with a neutral and indeterminate content – and the ICOs – which, as already mentioned, deliberately echo the institutional IPO while at the same time keeping themselves at arm's length – seem to be moving in parallel towards the same direction of freeing themselves from the heavy regulatory burden and from the costs of intermediation and information (in its various forms) to the market. This course of action requires a reaction – as has already been done in various national and supranational fora, as well as by different supervisory authorities – that goes beyond the thin shell that distinguishes such capital-raising operations and probes its underlying legal purpose (provided, of course, that there is a lawful one).

Leaving aside the hypothesis of tokens with a para-monetary function (payment/currency tokens), which *per se* fall outside the scope of financial markets law and are already the subject of other contributions within this volume, it is therefore preferred to focus the attention on two other macro types of tokens, those that according to the most common nomenclature are qualified *utility tokens* (or *vouchers*) and *security* (or *investment-type*) *tokens*.[5] Since tokens themselves are not suitable to express the rights associated with them, this is done by a document, usually called *white paper*, which, along

[4] With the clarification that the possible lack of standardization of tokens or their infungibility could in concrete terms prevent the exchanges, neither, as soon as will be seen, the nature of tokens always lends itself to the birth of a market.

[5] For the purpose of a minimal recognition and informative completeness, it is necessary to remember that between the economic-legal functions (exchange and participation) that polarize the qualifications indicated in the text there is a large set of hybrid tokens, which may enable their holders to benefit from the financial results expected from the implementation of the business project in which they have invested, or to achieve the goods or services provided. Not only that, tokens obtained at a certain stage of an ICO may have a purely prodromal character, as they contain only the right to be converted into other tokens issued to achieve the economic objective of the same, also automatically due to the occurrence of conditions deducted in appropriate smart contracts. Sometimes, then, tokens can apparently be devised as currency tokens, which, however, take on the substantive characteristics of utility tokens, being only usable as a means of access to goods/services provided by the issuer or, in any case, usable on the platform on which the offer has been perfected.

the lines of the information prospectus (but generally with greater brevity and clarity), is disseminated to illustrate the main aspects of the offer.

One is of the idea that all those virtual tools that rest on an exclusive (or, however, largely preponderant) commutative function should be classified as utility tokens: they, in other words, allow their subscriber to purchase an asset (present or future) or obtain a service from the issuer.

As such, they will allow the issuer to identify, as mere documents of title ("documenti di legittimazione": Art. 2002 Civil Code (hereinafter "CC")), the person entitled to the performance object of the contract, which will be regulated depending on the nature of the business project subsidized and accordingly to the relevant rules on a case-by-case basis (sale, procurement, licensing etc.). Another layer of rules shall also add up in the event that the subscriber acts as a consumer: in such a scenario, all relevant provisions of the Consumer Code (especially those contrasting misleading or aggressive commercial practices, those on unfair terms, those on pre-contractual information and distance contracts...) and Legislative Decree No. 70/2003 on e-commerce shall apply. From other points of view, the absence of a promise of financial returns or, at least, of an implicit expectation related to the investment, brings these tokens outside the scope of the Consolidated Law on Finance.[6]

Differently, security tokens can be variously fashioned to emulate the claims usually found in a wide range of investment vehicles, such as the right to profit participation or remuneration in the form of interest, and – even if this is irrelevant for the purposes of financial law – a more or less wide voting right may also be conveyed.

In the following paragraph, therefore, a few reflections will be devoted to these last instruments and to the problems that most closely concern them.

3. *Security tokens between company and financial market laws*

In the case of utility tokens, we have expressed a general preference for a subsumption under consumer law and this, it has to be added, is linked to the need to provide

[6] Even the application of a discount compared to the price of the promised good or service (similar to what happens in some variants of equity-based crowdfunding) does not seem likely to change the nature of the token in an investment: from an economic point of view, there will always be a financial component, but it is not reflected in the legal dimension, where, in the evaluation of the overarching contractual equilibrium, it is necessary to assess the centrality of the acquisition of a good or the procurement of a service in relation to the increase in capital invested over time. Therefore, in our view, the promise or the expectation of a profit has to be something *intrinsic* to the financial product and cannot be derived from the buyers' behaviour or anticipations, otherwise even a fungible material product could be easily qualified as an investment, depending on the reaction of market participants to its launch. For example, *utility tokens* issued by a smartphone manufacturer to boost the release of a much-anticipated new model of phone by offering some side benefit (privileged preview, special price discounts, access to custom made models…) may start an increasingly exuberant series of transactions (a secondary market of sorts) based on the hype of the announcement, as the day of the official launch gets closer. Nevertheless, the utility token cannot be converted into a security one based on this response, as it is completely unrelated to the rights attached to the token itself and to the issuer behaviour or activity. In addition, taking into account a subjective factor, such as the speculative attitude of some token-holders, could significantly contribute to blurring irreparably the boundaries of the definition of financial product by making it fundamentally unpredictable and variable, even within the very same issue of tokens, depending on individual intentions.

an adequate level of protection to the individuals that could find themselves in a condition of (cognitive, economic, etc.) inferiority or necessity, for the manner in which the offer is made to them and for the related profiles of technical and legal complexity, that could pay.

The background to this option is the protection of savings and the provisions of a high level of investor protection (Art. 47 Italian Constitution; Articles 12, 114 and 169 TFEU; Art. 38 Charter of Fundamental Rights of the EU) which constitute inescapable landmarks of the horizon of values in which regulators and interpreters must move in this matter.

This also applies to security tokens, where, however, it seems appropriate to carry out some further consideration on their qualification and on the identification of the conditions of legitimate use of this representational technique in the distinct – but closely related – domains of company (and negotiable instruments) law, on the one hand, and of financial markets law, on the other.

In the Italian legal system, it should be noted that the possibility of using the DLT to represent ownership interests, bonds or other debt instruments, and participative financial instruments (or mezzanine financing instruments) through tokens is subject to the preliminary and fundamental question whether this alternative technique is equivalent to the intertwined set of company rules and traditional paper-based negotiable instruments principles and, besides that, it is bound by a whole series of constraints.[7]

With regard to the first aspect, it does not seem possible to share an aprioristic and absolute rejection of "tokenization" because the answer inevitably depends on the heterogeneity and ductility of the DLT, as a technological framework – perhaps susceptible to further improvement – within which the creation, attribution and circulation of the token is realized. Thus, if the primary function of the DLT is precisely to create a shared register, as far as it is relevant here, it can be conceded in principle that resorting to DLT one can keep and update all those ledgers on which it is necessary to enter the information concerning company ownership interests, other securities and instruments that a company is entitled to issue (shareholders' register, register of bondholders, register of financial instruments holders...). From this point of view, the DLT has some features (almost simultaneous updating, inalterability of previous records, constant identifiability of holders...) that make it superior to the current techniques of keeping such books. Such a conversion could find its normative foundation in art 2215-*bis* CC, which legitimizes the use of IT for the creation and maintenance of those books, inventories, records and documents "which are to be duly kept by law or regulation or which are required by the nature or size of the business".[8]

[7] In approaching this question, we adopt an approach that takes into account the impetus given by economic and technological progress to the incessant regulatory evolution of credit securities. Over the centuries, their prescriptive nucleus has adapted from one representational medium to another, always reflecting the best technique available time by time in relation to the development of trade: as paper was at the time of the conception of the fundamental expedient of "incorporation", the scriptural recording (with its redundant superstructure composed of intermediaries with differentiated roles and in continuous interaction aimed at ensuring the coherence, uniqueness, exclusivity and irreproducibility of the titles circulating within it) has become the best option available later, to adapt to the explosion of market transactions, and now the DLT is beginning to occupy those spaces inaccessible for the cumbersome and expensive apparatus instrumental in dematerialization.

[8] It is not possible here to thoroughly demonstrate this argument, but one can imagine a systematic link between Art. 2215-*bis*, paragraphs 3 e 4, CC and Art. 8-*ter*, para. 3, Law Decree No. 135/2018, according

It is clearly not possible – nor, all things considered, useful – an uncritical "forward-fit" of the paper negotiable instruments principles in the modern, technological frame of DLT. Such an interpretative operation would be affected in its every statement by the repercussions of the begging the question (*petitio principii*) fallacy according to which the formalities inherent in the laws of circulation of paper negotiable instruments represent a general standard that is enforceable also outside the physical and tangible context from which they were originated and in relation to which they have been developed: Quickly, as it has already happened to some authors, one would be forced to find that it is impossible to comply with the paper-based formalities in the intangible DLT environment.

If, however, we bring the focus on the circumstance that Italian public limited companies ("società per azioni" – s.p.a.) can evade the shackles of paper materiality by opting for "the use of different techniques of legitimation and circulation" (Art. 2346, para. 1, CC),[9] then the appearance on the scenes of the DLT allows to overcome those strict schools of thought that recognized a minimum space to exercise private autonomy. DLT also helps to give an effective field of action to this rule, whose openness and receptivity enables technological innovation to take root within the legal system: we believe, in particular, that the DLT, if permissioned (specifically vesting the powers of control and modification in the board of directors)[10] and appropriately configured to

to which "the memorization of an IT document through the use of technologies based on distributed registers produces the legal effects of the electronic time validation referred to in Article 41 of EU Regulation no. 910/2014": thanks to this second rule, when its technical standards will be defined by the Agency for Digital Italy (Art. 8-*ter*, para. 4, Law Decree No. 135/2018), the DLT will allow the board of directors not only to keep the relevant company books, but to comply as well – and even more frequently – with the duties contemplated by Art. 2215-*bis* CC.

[9] Similar provisions that allow the definition of the law of circulation at the time of the issuance can be found in Art, 2346, para. 6, CC (for participative financial instruments, whose discipline also applies to "innovative start-ups" and to "innovative SMEs" established as "società a responsabilità limitata" (s.r.l., that is, a private limited company): Articles 26, para. 7, Law Decree No. 179/2012, and 4, para. 9, Law Decree No. 3/2015), as well as, even if more implicitly, in Art. 2447-*ter*, para. 1, let. *e*, CC (for financial instruments related to these segregated assets). It has to be pointed out, however, that most of the ICOs prohibited by the CONSOB consisted precisely in the offering of investments in which a promise of financial returns in the form of participation in the profits deriving from the issuer's activity was recognizable, according to a scheme which is very similar to a silent partnership or to a profit sharing agreement (i.e., precisely the kind of agreements that the doctrine has associated with participative financial instruments with great insistence). For bonds, debt instruments and debt securities of s.r.l. there are no rules that expressly allow the choice of alternative techniques of legitimation and circulation, but it seems that there are no insurmountable legal obstacles (also from the point of view of anti-money laundering provisions) to the digitalisation of the company books and to the transposition on a DLT of the key elements of the circulation of registered securities (consisting, in the absence of a paper certificate, in the possibility of submitting the transfers to the control of the issuer, ensuring the constant and unambiguous identifiability of the holder), or – even more easily – of bearer securities (characterized instead by the anonymity of the holders: this technique will therefore be forbidden where the professional underwriters are bound to guarantee the issuer's solvency: Articles 2412, para. 2, and 2483, para. 2, CC).

[10] A permissioned DLT system centered on the authority of the board of directors would also allow that board to make entries in the register of shareholders only vis-à-vis transactions carried out by persons and entities whose identity is certified through thanks to its digital identification (as legally provided) and after having verified if the transfer complies with the relevant articles of association (such as prior consent clauses, pre-emption clauses... possibly implementing a self-executing check of the required conditions via smart contracts – although this could imply facing substantial technical difficulties).

uniquely associate each token to the identity of a holder (also tracking down the sequence of previous transfers, pledges or encumbrances), permits to comply with the requirements imposed by the mandatory registration of shares in this new environment and to replicate the mechanisms underlying the attribution and exercise of corporate rights.

It does not seem, finally, that the issuance of "tokenized" shares can be assimilated to the case in which the company does not issue shares printed on paper certificates (Art. 2355, para. 1, CC[11]), thus giving exclusive relevance to the shareholders' register: conceptually, an entity that intermediates the relationship between shareholder and company still exists and the corporate autonomy may appropriately calibrate the system of assertable defenses (which, however, in the absence of a different provision, seem to include only the ones personal to the holder of the share/token and those common to all other holders of identical shares/tokens and not all those enumerated by Art. 1993, para. 1, CC: Art. 83-*septies* Legislative Decree No. 58/1998, "Consolidated Law on Finance" (hereinafter "CLF")), as well as preserve *bona fide* acquisitions[12] (in order to ensure maximum protection of buyers, even in a context of tendentially high security, such as DLT).

With regard, then, to the systematic constraints that preside over the representation of shares and ownership interests on DLT, it must be considered that: *a)* in the s.p.a. "tokenization" seems lawful only in the aforementioned scenario, and whenever the requirements imposing mandatory dematerialisation are not met (Art. 83-*bis* CLF), since the hierarchical and centralized architecture of this regime is incompatible with the functioning of the DLT; *b)* in the s.r.l. the improvident repeal of the register of members and the "outsourcing" of its functions to the Italian business register prevents a complete "migration" at company level to the DLT system.

[11] This article states: "In the case of lack of issuance of shares certificates, the transfer of shares will be effective vis-à-vis the company from the time it is entered in the register of the shareholders".

[12] Actually, a certain amount of criticism has emerged on the possibility that the good faith acquisition rule may be voluntarily reenacted resorting to contractual autonomy, but such a problem needs contextualization. We mean that the good faith acquisition rule was elaborated in an environment (the paper-based one) where historically it was felt a need to increasingly protect the position of the holder of a negotiable instrument against the issuer. In the first paperless environment, the dematerialised one, the lawmaker wanted to complete a process that had been started by the initiative of the private sector (during the '80s with the creation of "Monte titoli" s.p.a.) and foster a seamless transition to the new set of rules by salvaging as many preexisting ones as were fit to be adapted to a circulation system where materiality was banned. So, a new legal microsystem for dematerialised instruments was created (good faith acquisition rule 28 – 38 l. 213/1998, subsequently repealed and replaced by articles 82 et seq. CLF) along the lines of the previous one to eliminate the need for market participants to adjust to the logic of a completely new legal reality. After this passage was completed, it has to be noted that the good faith acquisition rule has *never* been applied, also because of the smooth functioning of the complex and centralized framework of professional operators. It seems now that DLTs are following a somewhat similar evolutionary path, abandoning their initial pioneerism to reach a phase of institutionalization: the only difference is that this new technology can leave the problem of the good faith acquisition behind, since in principle it allows a constant traceability of the holders and prevents the risks that the same good faith acquisition rule had been conceived to solve centuries ago. If it is possible to agree to this hypothetical presupposition, the fact that a high level of uniformity within DLTs is yet to be achieved should not *per se* prevent a jurist to consider that their further technical advancements could lead to a complete obsolescence of the good faith acquisition rule rationale of and ponder about the reasons why this could be a positive result: technology would have then solved a riddle posed by the material nature of negotiable instruments, granting a more secure circulation to their immaterial offspring.

In the latter case, the reintroduction on a voluntary basis of a computerised register of shareholders would, in most cases, increase the burden of formalities which, given the reduced circulation, could be easily carried out on a simple notebook. Moving now our sights onto the s.r.l. variants that are susceptible under Italian law to "go public" (such as "innovative start-ups", "innovative SMEs" and "SMEs"), the DLT could be a valid aid to mitigate some of the flaws of the alternative circulation system introduced by Art. 100-*ter*, paragraphs 2-*bis* to 2-*quater*, CLF, with specific regard to the possible ownership opacity resulting from the registers of "dematerialised" shares being entrusted to financial intermediaries. Indeed, a permissioned DLT, if homogeneously adopted by the issuer s.r.l. and by all the intermediaries, who are the registered holders of the shares, can greatly facilitate the identification of the actual members, the correct exercise of their rights (in lieu of the cumbersome and less secure issuance of a paper certificate) and the proper execution of sales orders (maybe on a platform created and run by the portal that managed the previous equity-based crowdfunding operation), which therefore would *ipso facto* be in writing.[13]

After these brief remarks on the systematic compatibility issues of security tokens within the frame of company law, the relationship with financial market laws will be dealt with now: in this respect, there is a widespread consensus on a case-by-case approach, with particular attention to the prevalence of substance over form, as this is, ultimately, the method most in line with the goal of maintaining a high level of investor protection. To this end, when it comes to qualify a token the Italian interpreter has to face a twofold option: *a)* to subsume it under the wider domestic category of *financial products* (Art. 1, para. 1, let. *u*, CLF), if all the known elements (the investment of capital, the assumption of a risk directly connected to it and the expectation of a financial return) which constitute it are present, or *b)* to classify it in the narrower category of *financial instruments* (a subset of securities at large), if a financial purpose is detectable and the token can be negotiated on the capital market (Art. 1, paragraphs 1-*bis* and 2, CLF).[14].

We cannot linger on the elements that would rather persuade to choose one qualification over another, also because it could turn out to be a lengthy exercise, destined to the immediate obsolescence due to the continuous adaptation process carried out by market operators; nevertheless, the consequences that can be derived are very relevant.

When a certain security token is eligible to be qualified as a *financial product*, the regulation on the appeal to public savings (Articles 94 et seq. CLF) applies and it becomes mandatory to draft and publish an informative prospectus; given the circumstances, also the rules on door-to-door selling (Art. 30, paragraphs 5 and 9, CLF) will be relevant.

On the other hand, if the conditions for the inclusion in the category of *financial instruments* are satisfied, the rules governing the provision of investment services (Art.

[13] This proposal, anyway, leaves unaffected the issue of the voluntary option in favour of such a system of circulation, which is left to the choice of the member, and it is likely to give rise to an undesirable discrepancy of circulation regimes simultaneously applicable, thus frustrating the original purpose of facilitating the formation of a secondary market.

[14] The negotiability of tokens is a prominent feature of DLT and in fact they are often meant to be exchanged on appropriate platforms (commonly known as "exchanges"), which already exist or are specifically created to serve this purpose.

1, paragraphs 5 et seq., CLF) will add up to those mentioned above; these services, notoriously, cannot be carried out without the prescribed authorisations.

It is therefore highly likely that the security tokens and the ICOs through which they are offered to the public will be brought back within the boundaries that they were designed to get rid of, unless the offers fall within the safe harbours provided for by MiFID2, by Articles 1(3) and 3(2) Regulation (EU) 2017/1129 of 14 June 2017 of the European Parliament and of the Council on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC, and, at the domestic level, by Art. 34-*ter* issuers regulation.[15]

And it is precisely the intersection of these safe harbours with the areas within company law where we have previously detected the possibility of a legitimate use of the DLT, which is mainly exploited by ICOs offering security tokens, filling the equity gap (where crowdfunding, ICOs' "ancestor", began to develop too): a no-man's-land where institutional investors are not interested to venture and the audience of potential investors is mainly made up of small savers. The greater part of the operations we are dealing with, actually, is addressed to these people, precisely because of the cheapness, immediacy and extensiveness with which the Internet can convey them.

If, on the one hand, this consideration leads us to agree with those who complain about the inadequacy of informational safeguards centred on the prospectus,[16] on the other hand, the substantial lack of progressivity of the protective apparatus of retail investors, that goes from vacuum to overload without effective graduation, which is particularly burdensome for smaller businesses and operations.

However, especially in front of an audience of small retail investors, enticed by the intuitiveness of online financial transactions, the apparent ease of acquisition and management of tokens and, above all, the promise of substantial returns, as mentioned in the beginning, the need for a high level of protection, cannot be abdicated, and it cannot be circumscribed to the prospectus alone, but must take shape at the level of the

[15] It is worth noting the exemption for the securities "issued with a view to obtaining the means necessary to achieve their non-profit-making objectives by associations with legal status or non-profit-making bodies, recognized by a Member State" (para. 1, let. *h*): apart from the questionable identification of the entities who can avail themselves of it, it does not exclude that such securities may also be associated with a prospective of financial returns (which, moreover, will be admissible only in cases covered by the special legislation), with the result that such issuances can be realized without quantitative limits and also using security tokens.

[16] The transparency paradigm was first flanked by that of investment professional intermediation with the MiFID and was then ousted from its primacy due to the more substantial and incisive consideration of the diverse needs of investor protection under MiFID2 by the more effective safeguards developed throughout the whole chain of production/distribution of financial instruments, thanks to the intervention powers given to supervisory authorities, and to the rules on internal organisation of the intermediaries themselves. In addition, with specific regard to the role of the prospectus (and its own comprehensibility), we can witness to its gradual override by the simplified informative documents sectorially introduced, as it has happened for the PRIIPs (Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs)) or in arts 23 and 24 of Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 [2020] OJ L347/1 (hereinafter "Crowdfunding Regulation").

activity of security tokens issuers and intermediaries, who cannot escape the requirements applicable to the provision of substantially equivalent reserved services, in accordance with the principle of technological neutrality.

It is not through the introduction of new categories of financial products or new investment services with the related special regulations,[17] anyway, that the problem can be adequately addressed, as has been done by certain states and territories (Malta, France, Liechtenstein, Gibraltar, etc.) in an attempt to steer a "Delaware effect" towards themselves: these selfish and uncoordinated incursions contribute only to the further fragmentation of the lexicon and syntax of financial markets law that should have been harmonized at European level, while even a superficial reconnaissance renders a rickety picture of discordant nationalisms.

Perhaps it is not even through the activation of innovation hubs and regulatory sandboxes at the supervisory authorities that one can trigger a reflection genuinely aimed at the objective of the highest level of protection for investors, since the stated purposes of these "laboratories" are to facilitate the testing of financial activities with a high rate of technological innovation[18] and that the interlocutors of the public institutions are, indeed, the operators who intend to carry out these activities.[19] Without then dwelling on the particularism that would also affect the results of similar experiences in the literally endless theatre of globalized finance, nor on the solidity of the architectures conceived within sandboxes, one cannot put aside the fear of a capture of the regulator, which not only watches, but creates itself (partly on demand) the conditions for the operation of the supervised, accompanies them in their artificial environment and determines the path after their exit.

Finally, due to the well-known slowness and rigidity of its legislative process, the European Union, on the one hand, has missed a good opportunity to integrate harmoniously the phenomenon of tokens in the regulation of crowdfunding, which represents the immediate precedent of the collection through ICOs and tends to involve the same set of recipients: in the recent Crowdfunding Regulation, in fact, there is only a fleeting

[17] Although this – it should be noted – was the option suggested by ESMA in its Advice of 9 January 2019 (*Initial Coin Offerings and Crypto-Assets*, ESMA50-157-1391) for non-financial tokens, also followed by CONSOB in its *Document for discussion* of 19 March 2019 and in the *Final Report* of 2 January 2020 (both entitled *Initial Coin Offerings and Crypto-Asset Exchanges*), albeit with specific attention to tokens that in Italy can be classified as financial products, and proposing that they were subjected to a specific regulation yet to be elaborated. Moreover, CONSOB proposed the adoption of an opt-in regime granting special exemption rules for ICOs issuers/offerors/promoters accessing dedicated platforms, but such a choice could be rather baffling for investors, due to the presence of other operators who can lawfully continue to operate outside them.

[18] In Italy, investor protection was considered in the introduction of regulatory sandboxes in the fintech field: Art. 36, para. 2-*bis*, Law Decree No. 34/2019 states that it is addressed "to *promote and support entrepreneurship*, to *stimulate competition in the market* and to *ensure adequate protection of consumers, investors and the capital market*, as well as to facilitate the link between institutions, authorities and operators in the sector [...]"). Nevertheless, its inclusion in this context, considering the potential players, seems destined to play a subordinate role.

[19] The institutional involvement of consumers' and investors' unions would not have been out of place, but they have been outright neglected.

trace of the renunciation to consider their inclusion.[20] On the other hand, the EU Commission[21] has published a complex and massive set of proposals addressed to implement various aspects of the *Financial Technologies Action Plan* (COM/2018/0109 final), with respect to which we simply raise the question of the benefit of the option in favour of a specific regulation of crypto activities, which could introduce a new category based on representational technique and not on the substance of such entities, thereby systematically marginalizing them. The situation, however, is still too premature to be able to express a more articulate judgment on this.

4. *Over the wall, chasing Sisyphus*

The answer to a complex problem – made so also by the enormous, labyrinthine and unstable body of financial markets law, a genuine legal *Gormenghast*[22] – can never be simple and it is even less so at a time in history when we are witnessing the advent of the underlying technology. In fact, if with its further progress the DLT will reach such a level of diffusion to supersede the technical equipment currently necessary for the proper functioning of the markets (regulated or not), then that will be a change of magnitude such as to involve a complete rethinking of the matter and no longer just a series of targeted changes, however problematic. Until then, though, the concern for the audience of potential small investors targeted by the ICOs requires the utmost caution, precisely because of the high percentage incidence that even small financial losses in absolute terms may have on their personal assets.

Many, therefore, are the initiative that could be taken, from the strengthening of the financial supervision to a general advancement of IT and financial culture, from the transplant in the digital field of the principles of customer relations to a reasoned rethinking of the structure and operation of intermediaries from the standpoint of technological neutrality… but they all need a common effort that transcends national particularities.

[20] Recital No. 15 of that Regulation states that "whilst initial coin offerings have the potential to fund SMEs, innovative start-ups and scale-ups, and can accelerate technology transfer, their characteristics differ considerably from crowdfunding services regulated under this Regulation". If one can agree that some variants of ICOs are conceptually distant and incompatible with crowdfunding, this certainly does not apply to security tokens and the motivation to leave them outside of Crowdfunding Regulation seems to be affected by an inadequate acknowledgement of the phenomenon, which is – to put it mildly – curious, given the detailed studies dedicated by other European institutions and agencies.

[21] We are referring to the Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937 (COM(2020) 593 final, intended only for crypto-assets other than financial instruments), the Proposal for a Regulation of the European Parliament and of the Council on a pilot scheme for market infrastructures based on distributed book technology (COM(2020) 594 final, aimed instead precisely at those crypto-activities classifiable as financial instruments and aimed at creating an experimental regime – the so called *Pilot Regime* – to be followed at a later stage by a comprehensive adjustment of the discipline of financial instruments),and, finally, the Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 (COM/2020/596 final, essentially prodromal and instrumental to the coordination of the *Pilot Regime* with other European legislation on financial, payment services and statutory audits).

[22] As the humongous and largely decaying fictional castle that is portrayed in the series of novels (*Titus Groan* (1946), *Gormenghast* (1950) and *Titus Alone* (1959)) written by the British author, Mervyn Pike.

In conclusion, the unevenness and sectoral nature of the innovations that each State claims to bring about (sometimes dangerously trying to anticipate future developments) are harmful both to the financial industry and to the "users" of its products. Only with a supranational coordination (made even more difficult by the outbreak of the COVID-19 pandemic) we can hope to develop a shared and genuinely harmonized regulatory framework that, after having defined sufficiently elastic and clear general categories, will be able to include ICOs and tokens in financial market laws and perhaps also to cope with other unexpected developments that the future holds.

At the same time, it will be necessary to avoid giving in to a superficial and unsystematic consideration, which reduces them to something new to *add*, rather than to *integrate* carefully, in this discipline. And this would be perhaps the most serious mistake, because as soon as the outlines of these umpteenth new boxes were sketched and their relationship with the rest of the financial legal framework painstakingly restitched, a new "wall" from which to escape would have just been built… so long to the protection of investors.

At that point, the boulder laboriously pushed to the top of the mountain will fall again downstream and we will notice the mocking look of Sisyphus, "who was the most cunning of men",[23] as he watches us go down to perpetuate his toil.

[23] *Iliad*, VI, 153.

SECTION 2

BLOCKCHAIN AND LEGAL IMPLICATIONS FOR PRIVATE LAW AND BUSINESS LAW

INTRODUCTION

THE BLOCKCHAIN TECHNOLOGY BETWEEN THE LAW OF CONTEMPORANEITY AND THE NEW POWER STRUCTURE

FRANCESCO GAMBINO

SUMMARY: 1. The aspirations of new technologies. – 2. Security, trust, shared consensus. – 3. An economic, political and legal instrument. – 4. Problems and prospects.

1. *The aspirations of new technologies*

Today, in the era of globalization, where are law-making processes generated? Who rules over the new phenomena produced by technology? What form does the law of contemporaneity assume in respect of these phenomena? These are the questions that have been absorbing the attention of jurists, sociologists and philosophers for over two decades. Contemporary society – increasingly disorganic and atomized[1] – suffers a perennial conflict between antagonistic forces. With the aim of prevailing over and subjugating other forces, these leverage the most powerful force available to Man today, namely technology, which is driven by modern science: "an effective power", intended as the "*form* of the actual production of specific and particular objectives".[2] The great technological revolution, in the widest variety of sectors (economic, financial, medical, military, etc.), aims to make human capital superfluous and ends up by deeply modifying the physiognomy of the world in which we live. Suffice it to think that a large part of stock market transactions is entrusted to algorithmic trading, that ever-smarter artificial intelligence systems are also designed to diagnose disease, that technology is used in settling controversies, and that the use of "hi-tech forces made up of unmanned drones" and computer viruses are "replacing the mass armies of the 20th century".[3] In this context, we wonder if law-making processes have moved from the law-making "centre", consisting of State institutions, to the "periphery", towards the confines between traditional law and other organized, autonomous and globalized social realms.[4] In this sense, the law ruling the new world manifests itself as a peripheral, spontaneous and social law.[5] On the one hand, free business initiatives defend themselves from public powers and, on the other, they build themselves as

[1] Byun-Chul Han, *Nello sciame. Visioni del digitale* (tr. F. Buongiorno, Nottetempo 2015), 27, grasps the most dismal aspect of *homo digitalis*: "the *socius* yields way to the *solus*; so, not so much a multitude as much as *solitude* is what characterizes the modern-day social form, which is overwhelmed by a general disaggregation of what is common and collective".

[2] E. Severino, 'Le domande del giurista e le risposte del filosofo' (2000) Contratto e impresa 665, 675.

[3] Y. N. Harari, *Homo Deus: Breve storia del futuro* (tr. M. Piani, Bompiani 2018), 376.

[4] G. Teubner, 'Regimi privati globali. Nuovo diritto spontaneo e costituzione duale nelle sfere autonome della società globale', in G. Teubner, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili* (tr. R. Prandini, Armando 2005) 57 ff., 61.

[5] Ibid. In these pages, I will give preference to the term "power" – peripheral, spontaneous, and social – rather than surrendering to semantically dilating the "juridical" phenomenon.

powers or sources of power.[6]

New social spheres, autonomous practices,[7] private legal orders[8] take shape and are structured by exploiting technological resources which offer innumerable opportunities, meet the immediate need for certainty and are capable of sterilizing and settling conflicts. These powers are established with the consensus of those who acknowledge their reliability and who use them in different sectors to achieve specific and particular aims. The safety – and immediacy – of this instrument, trust and shared consensus are the principal features of a peripheral, spontaneous and social power. This power, by offering what the State is unwilling or incapable of offering, spreads throughout the community, coming into competition with the traditional forms of exercising political and legislative power, and invading the field of law-making processes. This gives rise to the dispute on the very concept of "legality" that appears to be contended between conflicting *powers* which, through their conditioning and prescriptive nature, *de facto* assume the authoritative force of a legislator.

2. *Security, trust, shared consensus*

Security, trust, and shared consensus are the soundest grounds on which a power – the power of technology – could lie as it manifests and concretizes without waiting to take the form, structure and apparatus of traditional law. It is in this setting that the Blockchain technology – by assuring security, calculability and reliability – offers unlimited potential in the widest variety of sectors.

Blockchain (literally "chain of blocks") is a technology based on DLT (Distributed Ledger Technology) in which data is grouped in "blocks" that are interconnected in a time sequence through shared consensus mechanisms. It is comparable to a digital register or ledger in which every transaction is validated through a shared process in which participants receive a copy of each operation. As soon as the blocks are created and validated, they are closed and "linked together" sequentially and, in this sense, can be defined as crystallized in time, thus becoming unalterable. It is an instrument that enables the storage of the transactions closed, securing them against the risk of external manipulations or tampering. This technology was developed in two different phases. The first focused on the dealing and trading of *cryptocurrencies*; the second was aimed at pursuing other objectives by means of a distributed *software*, also known as *smart contracts*.[9] It might be useful to reflect on the fact that the monetary function of cryptocurrencies – that marked the first phase of Blockchain's development – is ensured not by the trust placed in an issuer but by the trust placed in a sort of "acephalous" predefined technical issuance process.[10] It should be pointed out that in

[6] N. Irti, 'Tramonto della sovranità e diffusione del potere', in A. Febbrajo and F. Gambino (eds), *Il diritto frammentato* (Giuffrè 2013) 3 ff., 13.

[7] On the unlimited number of models of order that distinguish the typically post-modern vision of the world, see Z. Bauman, *La decadenza degli intellettuali. Da legislatori a interpreti* (tr. G. Franzinetti, Bollati Boringhieri 2007), 14.

[8] G. Teubner, 'Ordinamenti frammentati e costituzioni sociali', in A. Febbrajo and F. Gambino (eds), *Il diritto frammentato* (Giuffrè 2013), 381-382.

[9] G. Gitti, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca, borsa e titoli di credito*, 2020, p. 13.

[10] M. Cian, *La criptovaluta - Alle radici dell'idea giuridica di denaro attraverso la tecnologia*: *spunti preliminari*, in *Banca, borsa e titoli di credito*, 2019, p. 318.

this case what creates trust in the community members is a technological tool – and not a superordinate power – testifying to its spontaneous, autonomous and self-organized creation.

It might be useful to briefly outline some of the aims and characteristics of Blockchain-based technologies: a) reduce the cost of transactions by eliminating intermediaries and intermediation costs; achieve organizational efficiency through a reliable decentralization process; b) feature encoding and control mechanisms capable of "democratizing" data and building confidence as they are assured by cryptographic algorithms through a secure transaction validation and storage mechanism; c) provide the immutability and inalterability of data storage; d) assure transparency, traceability, security; e) ensure the pseudonymization of users, timestamping, and asymmetric cryptography. By modifying trust-placing mechanisms, Blockchain applications have radically transformed value transfer methods. These applications, in a wide range of sectors, may involve public networks, energy markets, transport, the healthcare sector, supply chains, education, creative industries and copyright and the financial sector.

3. *An economic, political, and legal instrument.*

In the light of European Union legislation and national laws, legislators cannot remain indifferent to the sensational resources offered by the Blockchain technology. The European Parliament, with a view to building trust through disintermediation, passed a Resolution on 3 October 2018, in which it took a stand on distributed ledger and Blockchain technologies. The Resolution starts out by stating that Blockchain can be used in very a large number of sectors and does away with intermediation costs, thus constituting a useful tool "that promotes the empowerment of citizens by giving them the opportunity to control their own data and decide what data to share in the ledger, as well as the capacity to choose who else can see them".[11] In this perspective, Blockchain not only sums up to an economical technological tool but to a tool that is also endowed with a political nature: both because it aims to "democratise data and improve trust and transparency, providing a secure and efficient route for the execution of transactions"[12] and also because it is intended to promote a "self-sovereign" digital identity through which DTL technology could generate "the emergence of new models to change the current concept and architecture of digital identities".[13]

From the standpoint of Italian national legislation, Art. 8-*ter* of Decree Law No. 135 of 14 December 2018, converted into Law No. 12 of 11 February 2019, defines distributed ledger-based technologies and outlines the characteristics of *smart contracts*, laying down some of their legal effects and referring the regulation thereof to the Guidelines issued by the Agenzia per l'Italia digitale – Agency for Digital Italy (AgID). More specifically, *smart contracts* provide: a) an "automatic" contractual tie deriving from the execution of *smart contracts*;[14] b) the equivalence between the requirements of the written form and the "requirement-fulfilling process" laid down in

[11] European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), P8_TA(2018)0373.

[12] Ibid.

[13] Ibid.

[14] Art. 8-*ter*, para. 2, Decree Law No. 135 of 14 December 2018.

the Guidelines of the Agency for Digital Italy;[15] c) the equivalence, in terms of legal effects, between the "storage of a digital document through the use of distributed register technologies" and "electronic time validation".[16]

4. *Problems and prospects*

The dialectics between the law of contemporaneity and the new decentralised powers, driven by widespread trust and shared consensus, turns more controversial and stringent in several phenomena that will be closely analysed in different realms of study in the different contributions to this section. First and foremost, there is the problem of *legal certainty.* The security – and infallibility – of technological automatisms per se does not and cannot express the certainty of law. In this respect, it is necessary to make a distinction between the investigative approaches and the points of view from which these phenomena – the technological and the legal – may be observed. Let us start with the force – at the same time entrusting and persuasive – of the Blockchain technology, which rests on its capacity to express calculability, regularity and stability. In this sense – namely the sense of security created by this instrument by generating trust among its users – Blockchain expresses much more than the continuous succession of two facts schematized into a law.[17] In other words, precisely by virtue of its sure and immediate functionality, this technology can be compared to causality in natural law by making almost *certain* the probability of the effects consequent to specific facts. However, as it is the legislator who decides the *legal* consequences of our behaviours – also in digital environments – in many points of the Resolution of 3 October 2018, the European Parliament urges the Commission's attention thereto. With reference to smart contracts, the text "stresses that the Commission needs to undertake an in-depth assessment of the potential and legal implications"[18] and clarifies that "legal certainty surrounding the validity of a digital cryptographic signature is a critical step towards facilitating smart contracts".[19] In this context, it is a call to the legislator's sense of responsibility. Although the characteristics of the Blockchain technology represent the elements of a self-structuring power, they cannot stand without normative support. They need to be coordinated with legal orders, at national and supranational level, which only laws can assure. For automatisms, processes and technological devices to work in a legal system – and thus gain access to protection mechanisms and to the possibilities offered thereby – they need the nexus of causation or of legal imputation to reconnect the *effects* that typically express and distinguish the law to the events and the outcomes of the realm of technology.

[15] Ibid.

[16] Art. 8-*ter*, para. 3, of Decree Law No. 135 of 14 December 2018). See also Art. 41 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[17] With the consequence of comparing a fact with the first term of the Law ("if A") knowing that another fact complying with the second term ("then B") must occur. On the reasoning of Flavio Lopez de Oñate, see the considerations by F. Carnelutti, 'La certezza del diritto (1943)', in G. Astuti (ed.), *La certezza del diritto* (Giuffrè 1968), 200, which focus attention back on the contrast between the certainty of law and justice.

[18] European Parliament Resolution of 3 October 2018 (n 11).

[19] Ibid.

Thus, for example, even if the Blockchain information system is inalterable, transactions are secure and the data storage is effortless – elements undoubtedly useful to a notary public – within the framework of applicable laws, it is improper to compare the concept of notarization with the results achievable through the use of Blockchain technology. It suffices to reflect on the terms of this comparison.

While Blockchain boils down to a decentralized information system – that does not include intermediation – according to the law, the activity of a notary is the expression of the centralization of the State's public function.[20]

Then there is the issue of *traceability.* If, on the one hand, the Blockchain technology can offer visibility and transparency as a *protective function,* solving the problems of food traceability by managing the entire life-cycle of food products;[21] on the other hand, it can generate forms of opacity and concealment with respect to identifying the subjects on the supply chain. The question of traceability raises relevant issues in operational terms and at political and legislative level. In this introduction, we can list two. At operational level, the resources of "DLT can provide a framework of transparency, reduce corruption, detect tax evasion, allow the tracking of unlawful payments, facilitate anti-money laundering policies, and detect misappropriation of assets".[22] At political and legislative level, it is instead necessary to make an in-depth analysis of whether the use of DLTs complies with UU legislation on data protection and in particular with the General Data Protection Regulation (GDPR).[23]

Lastly, note should be taken of the phenomenon linked to the problem of legal certainty connected to *contract automation* in a digital single market. The European Parliament Resolution of 3 October 2018 highlights the relevance of DLT-enabled "smart contracts" that "can act as a key enabler of decentralised applications", by hopefully monitoring the use-cases in order to explore the potential of these instruments, calling on the Commission to promote the development of technical standards and to conduct an in-depth analysis of the existing legal frameworks in the different member States.

This scenario opens the perspective of various and multifarious applications of the Blockchain technology. Suffice it to think of corporate law. In addition to the possibility of easily identifying shareholders and of introducing the automatic enforcement of corporate rules, it opens a path towards organizing decentralised autonomous infrastructures to use platforms capable of providing dispute resolution mechanisms and of making a broad use of *smart contracts*.[24]

These last research approaches have led to a conclusion that can offer even more food for thought. The key issue is the continuity that can be recorded between the new digitally-generated contractual "mechanisms" and supranational law.

As has been pointed out, with the Resolution of 3 October 2018, the European Parliament promotes the use and spread of "smart contracts" throughout the digital single market insofar as they are instrumental to spreading decentralized applications. Within this framework, the European Parliament notes, however, that "legal certainty can be enhanced by means of legal coordination or mutual recognition between

[20] See, in this Section, the contribution by E. Damiani.

[21] See, in this Section, the contribution by P. Lattanzi and S. Mariani.

[22] European Parliament Resolution of 3 October 2018 (n 11).

[23] See, in this Section, the contribution by E. Pederzini.

[24] See, in this Section, the contribution by F. Möslein.

Member States regarding smart contracts".[25] Here the law is once again pressured by questions on the sense of the philosophy of law. The network of the *lex mercatoria* – and, in this context, let us add the network of the *lex digitalis*[26] – "in addition to subsuming the regulation of civil society in the different Countries", ends up extending to "the very international political relations", thus turning the "deified" form of the contract[27] into a possible "*rootless* law", as the "foundation of the only Order possible in the era of never-ending transformations".[28]

[25] European Parliament Resolution of 3 October 2018 (n 11).

[26] Teubner (n 4), 381.

[27] In this context, this form expresses itself and sums up in the coordination and mutual recognition between member States as hoped for by the European Parliament to develop a common regulation of "smart contracts".

[28] M. Cacciari, *Il lavoro dello spirito* (Adelphi 2020), 18. A *rootless* law can exist "only in a 'deified' form of the contract whereby the very relations between political powers are conceived within its order and subordinated thereto" (Ibid., 17-18).

BLOCKCHAIN APPLICATION IN GENERAL PRIVATE LAW: THE NOTARCHAIN CASE

ENRICO DAMIANI

SUMMARY: 1. The open (or pure) Blockchain. – 2. The permissioned (or closed) Blockchain. – 3. The Notarchain. – 4. Scopes of the Notarchain. – 5. Final evaluation.

1. *The open (or pure) Blockchain*

It was singled out[1] that the *Blockchain* is a technology able to keep, in a reliable way, a system of registers suited[2] to preserve an indelible and unmodifiable sign of given operations; limiting the analysis within the field of private law,[3] a first aspect to analyse is the one related to the transfer operations without any interventions by a centralized authority that can relate to virtual currency or any other type of goods.

In the open (or pure) version the *Blockchain* does not show any access hindrance, there are no qualified fiducial issues and the final recipients of the subjective legal statuses directly have the cryptographic keys enabling to have the same legal statuses available[4] that can be: self-representative, as in the case of the *Bitcoins* existing inside the *Blockchain*, that is being representation of the existing physical proprieties outside the cryptographic representation (*off-chain*) which is in such a case a simple *token*, a kind of symbol representing the goods and which can circulate thanks to the *Blockchain*.

In the case of a *token* circulation the biggest problem[5] to be faced is how to guarantee the correspondence between the physical good and the *token* itself. For example, in the case of the transfer of a real estate, it often happens that this latter is

[1] U. Bechini, *Il notaio digitale. Dalla firma alla blockchain* (Giuffrè 2019), 152 ff.; B. Arruñada, 'Blockchain's struggle to deliver impersonal exchange' (2018) 19 Minnesota Journal of Law, Science & Technology 55. The reflections by T. W. Dornis, 'Artificial Creativity: Emergent Works and the Void in Current Copyright Doctrine' (2020) XXII Yale Journal of Law & Technology 1, are very interesting and possible to be shared.

[2] About the potentialities that the Blockchain could express within Civil Law see A. Borroni, 'Blockchain: Uses and Potential Value', in A. Borroni, *Legal perspective on blockchain theory, outcomes, and outlooks* (Edizioni Scientifiche Italiane 2019) 5.

[3] The arrival of new technologies seems to have undeniable problems on the whole system of Private Law, both on companies and on fundamental rights and freedoms. See M. Giaccaglia, 'Considerazioni su Blockchain e smart contracts (oltre le criptovalute)' (2019) 35 Contratto e impresa 941; D. Di Sabato, 'Gli smart contracts: robot che gestiscono il rischio contrattuale', in G. Perlingieri and A. Fachechi (eds), *Ragionevolezza e proporzionalità nel diritto contemporaneo* (Edizioni Scientifiche Italiane 2017) 387 ff. For a more recent paper, see E. Caterini, *L'intelligenza artificiale "sostenibile" e il processo di* socializzazione *del diritto civile* (Edizioni Scientifiche Italiane 2020) 11 ff., 42 ff.

[4] Bechini (n. 1) 153.

[5] There are many problems linked to the use of new technologies. See V. Moscon, Tecnologie blockchin e gestione digitale del diritto d'autore e connessi' (2020) Il diritto industriale 137; M. Fink, *Blockchain regulation and governance in Europe* (Cambridge University Press 2018); G. Rinaldi, 'Smart contract: meccanizzazione del contratto nel paradigma della blockchain', in G. Alpa (ed.), *Diritto e intelligenza artificiale* (Pacini Editore 2020) 343 ff.

apt to changes (a plot of land becomes a building, a one-storey structure is raised to two etcetera). We are not facing unchanging entities like the *Bitcoin* so it should be necessary to think up a method enabling either to modify the *Tokens* or to give some more in addition.

The problem linked to the risk of losing the cryptographic key corresponding to a given legal status is of a no lessen importance. In such a case there would be the loss of the juridical control and the availability of the status itself.[6]

But also with reference to the legal statuses called self-representative as in the case of the *Bitcoins* there are some relevant problems coming to light: for example the anonymity enables the execution of huge patrimonial transfers with no possibility of identifying the subjects of the relationship with an evident risk of the possibility of performing criminal operations. In addition, the impossibility to identify the users in the open *Blockchain* makes the refund type remedies almost impossible to be performed as it is said that it "lives in a legally void space".[7]

Even disregarding intents of a criminal kind, it is undeniable the use of the *Bitcoins* that could be made by someone who would like to avoid the aggression of the Revenue Office, or of his creditors, or of a spouse who is the beneficiary of an alimony cheque etc. Whether even the real estates could be transferred through a pure *Blockchain* one could imagine an equally dangerous use of such a technology in order to satisfy individual and egotistic questionable interests.

2. *The permissioned (or closed) Blockchain*

Instead of the open *Blockchain* showing the above-mentioned critical conditions, the creation of a *permissioned Blockchain* (or closed) is possible by a group of people according to the conventionally chosen rules related for example to the singling out of the involved operators, the way to insert data, the settling of possible disputes, etcetera, which is basically immune from the risks of the first one.

The operators can make use of technical precautions aimed at avoiding that the digital data, necessary for the *Blockchain* management, can be lost and are able to activate some mechanisms suited to eliminate negative economic effects arising from the failed correct functioning of the system,[8] also through entering insurance contracts.

In a closed *Blockchain* the involved people are identified and the operations they carry out will be perfectly tracked; the related data will be legally binding due to the initial convention and all the operations will be subject to the private international legal system. Notwithstanding this, recurring to such a technology will always be a convenient operation, for example for the costs linked to need of maintaining more knots and therefore more computers, interconnected among them, through a demanding economic investment in comparison for example to a centralised database.

[6] Bechini (n. 1), 155, who, to state the seriousness of such a possibility, recalls the American saying "Grandma picks a bad password and loses her house" quoted by J. Kaufman Winn, 'The Hedgehog And The Fox: Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions' (1999) 51 Administrative Law Review 955.

[7] Bechini (n. 1), 158.

[8] Ibid., 161.

Resorting to the Blockchain has also been suggested to replace the already existing centralised systems.[9]

Think about the Blockchain for real estate adverts: some particularly qualified subjects, called *Gatekeepers*, would have the task of checking the transfer deeds, eventually filing them in a *ledger*.

Arruñada investigated the value the blockchain can add to the transfer processes in the real rights of real estates, exploring its potential and stigmatising the main difficulties that should be faced. He states that, contrarily to common statements proclaiming the end of mediators and the involvement of the States, the possible application of the blockchain in such a sector will have to make use of some specialists including public officials, especially for real estate transactions.

3. *The Notarchain*

Notarchain is a project aimed at the creation of a new platform that uses blockchain technology through the implementation of a series of proven open source technology protocols that will consent the transfers of goods and rights, their registration and archiving, in an easy way, quickly, safely and without high costs.

It has been possible to design the "Notarchain" project after the issue of Law Decree No. 135 of 14 December 2018[10] stating the urgent provisions about the support and the simplification for the companies and the public administration (the so-called "simplification decree").

The simplification decree introduces the definition of DLT: *distributed ledger technologies* in the set of rules, defining what the *smart contracts* are and foreseeing, if some requirements are met, that the same ones are compared to written contracts; finally it compares to the time stamp foreseen by the eIDAS Regulation (*electronic IDentification Authentication and Signature*)[11] on the electronic identification the *timestamp* on the DLT meeting the requirements identified by the Agency for Digital Italy (Agenzia per l'Italia digitale (AgID)).

Those provisions realise an official link between the legal system and the distributed ledger technologies (DLT) enabling this way the resort to the Blockchain functions.

The simplification decree foresees an equivalence between the *time stamp* of the blockchain to the time stamp in order to create a juridical certainty about the stamp applied to the digital document.

Some political parties stated it is a "notarization" phenomenon on a large scale, but such a reference seems rather wrong.

First of all, it is not correct to talk about "*notarization*" as the application of the *time stamp* is not certainly such and also because such a technique of time validation has been existing for long in our legal system. The idea that through the blockchain

[9] Ibid.

[10] Decreto-legge 14 dicembre 2018, n. 135, Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione, in *Gazzetta Ufficiale della Repubblica Italiana* No. 290, 14 December 2018.

[11] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

one can get juridically equivalent results to those obtained through the resort to the Notary registration is wrong. The concept of "*notarization*" applied to the *blockchain* expresses the idea of providing a certain date and to make some information unmodifiable.

No true notarization is currently feasible through the blockchain both for the regulation context created through the simplification decree and because the compatibility between the Notary activity and the features connected to the blockchain is totally uncertain. The blockchain represents a system of information registration that is decentralised and with no intermediation, while the Notary activity is the expression of the centralization of the public function being the public officer the subject appointed to ascribe public trust to a document.

Notaries have immediately shown their interest for the "*distributed ledger technologies*" (DLT) keeping the distance from the so-called permissionless blockchain (*pure*, therefore distributed on many knots with no hierarchy).

Notarchain is a project by the National Board of the Notaries launched in 2017 and it foresees a *permissioned*, closed structure where the validation is reserved to a restricted core group of knots particularly qualified. The goal of the project is to guarantee safety in transactions, in partnership with IBM, is that of answering to the needs of digitalisation of the State and to guarantee the safety of transactions

Three relevant aspects[12] concerning *Notarchain* have been singled out: first of all the information will be handled not by anonymous subjects but directly by Notaries; the used platform will enable swiftness in acquiring information and keeping the registers, without any costs for the citizens, with the possibility of storing data at a world level, without the related difficulties linked to a decentralised data collection; finally safety will be highly implemented through the impossibility to modify the data, the previous check of the identity of the subject involved and the "correctness and completeness of the same data inserted in the chain".

Being basically a digital base of storing and managing files, it will be possible to extend its use to different applications.[13]

4. *Scopes of the Notarchain*

An example of application of the Notarchain[14] is the creation of a Public Register aimed at making the deeds for the appointment of Guardians known: the platform designed by Notartel S.p.A., a company of the National Register of Notaries and the National Fund of the Notaries providing IT services to Italian Notaries, guaranteeing them the access in real time, and on which it will be possible to insert the essential

[12] G. Gatti, *Notarchain, la blockchain dei notai* <https://www.giuseppegatti.it/notarchain-la-blockchain-dei-notai.html>.

[13] S. Amadori, *Arriva Notarchain: la Blockchain tutta italiana* (18 November 2017) Blockchain4Innovation <https://www.blockchain4innovation.it/mercati/legal/smart-contract/arriva-notarchain-la-blockchain-tutta-italiana>.

[14] The examples of application of the Notarchain were assumed by G. Marcoz, *Notarchain* <http://www.gestitec.polimi.it/it/risorse/file-pubblici/proptech-monitor-italia-novembre-2018/notarchain> and by E. Signori, 'Notaio e Blockchain', in G. Alpa (ed.), *Diritto e intelligenza artificiale* (Pacini Editore 2020), 401 ff. About the possible uses of the blockchain in business law, see the recent contribution by N. De Luca, 'Documentazione crittografica e circolazione della ricchezza assente' (2020) Rivista di diritto civile 101.

data of the deed of the appointment of guardians. The content of the register can be singled out and shared by Notaries and by other qualified subjects, like local health authorities. Such a system can be used also for the registers of proxies, of oleographic wills, of advance directives for the treatment and will about the donation of organs.

Another project that is under development is the compiling a unique register of the professions based on the blockchain (AUP is the Italian acronym), thought to uniform the different database existing today. Such a Register would enable the realisation of an integrated system suited to make it possible to share qualified information, as the role of someone registered in a Roll, guaranteeing full autonomy to the Rolls the subjects belong to for the management of the information ascribed to them.

The way for consultation is standardized and it can be used by telematic IT applications and the system enables the ongoing update of the role/qualification of each registered professional.

The Register is made up naturally by as many knots as the bodies entitled for the issue of the registrations and the license to practice to the Professional Rolls; they are the only entitled subjects for keeping the archive while those that are involved in the consultation of the Rolls can register to the net, simply having the permission of reading the data searched for.

Another project called "COMMODITIES OF THE PUBLIC SALES DEED" foresees the involvement of the Notaries, of the Public Bodies and of the operators of the sector like the real estate agencies and the managing agents and it is aimed at enabling the automatic transition of information linked to notary deeds (registered residence, bills of the utilities, taxes on the garbage disposal, the estate charges, the ones for the condominium, etc.) in order to enable the creation of a more effective and faster system of disintermediation of the information.

One of the projects that is being studied is the one called "MONNALISA" where the Notaries, the technological partner and the Cultural Heritage Ministry are involved. The core matter of such a project is making virtual and certifying any single work of art and the creation of a certified system for transferring the works of art.[15]

The objective is the one creating a safe system, clear, official of assignment of valuable moveable proprieties. A system based on the Blockchain technique can enable the access to every artist by registering his/her works and therefore the rights on his/her creations, obtaining that way a digital sealing of the data inserted that cannot be altered afterwards[16]. Such a register could be used either by auction houses or by the single collectors to know the legitimate origin of a work of art, the previous transference of the same one with the related quotation and so on.

The Law Decree No. 109 of 28 September 2018[17] foresaw in clause 14, para. 4, that the Ministry of Cultural Heritage had an extraordinary national plan for monitoring and preserving the real estate belonging to the cultural heritage, fixing the criteria for their singling out also to submit them to interventions for their conservation, establishing the instrumental control systems to be used for the monitoring activities[18].

[15] Giaccaglia (n. 3), 966-967.

[16] Ibid., 967.

[17] Decreto-legge 28 settembre 2018, n. 109, Disposizioni urgenti per la città di Genova, la sicurezza della rete nazionale delle infrastrutture e dei trasporti, gli eventi sismici del 2016 e 2017, il lavoro e le altre emergenze, in *Gazzetta Ufficiale della Repubblica Italiana* No. 226, 28 September 2018.

[18] Giaccaglia (n. 3), 964.

It is possible to imagine that the mapping of the estates under the historic and artistic interest can happen thanks to a digitalised system inserted in a *blockchain*.

Another project that is worth considering is the one called "BITCOINA", which involves the Notaries, DEVO lab by SDA Bocconi and a technological partner having the realisation of a platform as its goal, which could supply the "notaries" with controls in case of transference of virtual currency in order to give life to a safe and clear system for the virtual currency transactions.

With the crypto currencies[19], regardless the safety features implicit in the same blockchain technology, there are often cases of theft, loss or involuntary cession involving the storing and transference systems and the sales platforms.

In these cases, if the password used by the user to manage and validate the operations gets lost, the user can no longer sign the transaction unless the service is developed in multisig, for which the signature of a third validating subject is necessary, and this can be the Notary indeed in order to ensure safety, avoiding thefts and guaranteeing the real will of the parties in the transference.

Another fundamental problem concerns the identity of the user[20], that being represented only by an alphanumeric code ensuring anonymity, is openly in contrast against the current anti-money laundering legislation. The Notaries could be the grantors of the identity of those operating on the public blockchain.

A further field where the role of the Notaries could be used is made up of escrow[21] services to execute completely the *smart contracts*.

The *escrow agreement* is a popular contract in the *common law* systems that is spreading also in our set of rules through which the parties entrust a third subject by means of a proxy to manage a cession of movable and immovable properties, including the assignment of shares and the companies or their branches. Following the entering of the *escrow account* agreement, the contracting parties entrust the third party with the propriety or the document that is the core matter of the economic operation and its countervalue in money. The entrusted propriety and the amount filed are managed on behalf of the entrusting parties until a given condition set forth by the parties takes places to be finally entrusted to the one entitled.

A third party that might be a Notary, therefore acts as an *escrow agent* among the contracting parties.

There are several useful points for resorting to such an institution: the amounts merging in the deposit are no longer available for the depositor and they can be enforced against the creditors, even in case of bankruptcy of the grantor; the creation

[19] G. Gatti, *Dalla blockchain, la notarchain per la validazione di contratti* <https://scienzamagia.eu/world-wide-web/dalla-blockchain-la-notarchain-per-la-validazione-di-contratti>; Signori (n. 14), 410, correctly notices how the intervention of the Notary in the role of controller and manager of the signatures for the use and the exchange of cryptocurrency through "multisig" services is beneficial, everything by subordinating any operation to the use of the digital signature to make the transactions safer and clearer.

[20] About the topic of digital identity see: G. Alpa, 'L'identità digitale e la tutela della persona. Spunti di riflessione' (2017) Contratto e impresa 723; G. Resta, 'Identità personale e identità digitale' (2007) Il Diritto dell'Informazione e dell'Informatica 511; A. L. Tarasco and M. Giaccaglia, 'Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo' (2020) Il Diritto dell'economia 270; Signori (n. 14), 410.

[21] G. Quatraro and R. Israel, *L'escrow agreement e il ruolo del notaio* <https://www.federnotizie.it/lescrow-agreement-e-il-ruolo-del-notaio>.

of an *escrow account* can represent a guarantee for importing companies and such a technique is finally much appreciated by banks and insurance companies to issue guarantees to the companies.

5. *Final evaluation*

As we have to summarise this short research aimed at highlighting the possible interactions between the blockchain and the Notaries, inverting what is the usual approach of a survey, it is now suitable to develop some general reflections.

The history of technology is strictly linked to the history of contracts[22]. In the dissertation for his Degree then published in the journal *Il Filangieri* in 1901[23], Antonio Cicu faced the topic of the importance of robots in private law, in particular analysing all the problems linked to the signing of the contract through the help of mechanic devices and trying, successfully indeed, to systematically focus those particular cases within the general subject of the contract as it can be extracted from the Civil Code dated back in 1865.

Many of the hints and reflections of the interpretation of that time, in particular the German and the Italian ones[24], can be to a large extent reconsidered and deepened in order to verify their newness also with reference to the bracketing born after the technological innovation of the last ten years[25].

Part of the interpretations[26], with a particular reference to the case of finalising contractual operations through the use of new technologies, questioned the consequences that the lack of dialogue between the parties can create in the same singling out of the categories of the so-called exchanges without agreement, where the contract would come out from the combination of two juridical deeds, often due to *per facta concludentia*, without being able to amount to a true agreement in any way.

The development of cybernetics, that branch of the science determined to study and realise the study and the realisation of suitable devices and machines to simulate the functions of the human brain, self-regulating through signals of power and control either in electric circuits or in mechanic systems, determined the increase of the research concerning the so-called *software* agents that is those "smart" programmes able to perform the interaction with a given level of autonomy, spontaneous

[22] Rinaldi (n. 5), 343, who recalled a concept eminently recalled by N. Irti, *Norme e luoghi. Problemi di geo-diritto* (Laterza 2006) 187.

[23] A. Cicu, 'Gli automi nel diritto private' (1901) Il Filangieri 561 ss., an essay fully quoted in *Scritti minori di Antonio Cicu*, II, *Successioni e donazione – Studi vari* (Giuffrè 1965), 287 ff.

[24] W. Auwers, *Der Rechtsschutz der automatischen Wage nach gemeinem Recht* (Göttingen 1891), 5 ff.

[25] Let me refer to E. Damiani, 'Note in tema di conclusione del contratto mediante sistemi automatici (spunti per una rilettura delle tesi di Antonio Cicu)' (2020) Rassegna di diritto civile 747.

[26] N. Irti, 'Scambi senza accordo' (1998) Rivista trimestrale di diritto e procedura civile 347. This work was followed by the criticism by G. Oppo, 'Disumanizzazione del contratto?' (1998) Rivista di diritto civile 525, followed by the reply by N. Irti, 'E' vero ma…" (replica a Giorgio Oppo)' (1999) Rivista di diritto civile 273; as well as the criticism by C. M. Bianca, *Diritto Civile. Vol. III – Il contratto* (Giuffrè 2000) 43 ff. To which there was the counter-reply by N. Irti, 'Lo scambio di foulards (replica semiseria al Prof. Bianca)' (2000) Rivista trimestrale di diritto e procedura civile 601, to which there was the reply by C. M. Bianca, 'Acontrattualità dei contratti di massa?' (2001) Vita notarile 1120; F. Gazzoni, 'Contatto reale e contatto fisico (ovverosia l'accordo contrattuale sui trampoli)', in *Studi in onore di C.M. Bianca* (Vol. III, Milano 2006) 313ff.

interaction in complex environments, such as the search for information in the web, the interaction with possible human or artificial counterparts autonomously and without external requests[27].

Recently the European Bank for Reconstruction and Development has published a study[28] on its website where, trying to give the legislators of the European States members some guidelines about *smart contracts*, it interestingly questioned about, for example, the possibility of introducing the concept of "electronic person" with reference to the *automated software* able to finalise contracts autonomously, basing on the models of artificial intelligence and *machine learning*[29] techniques.

If it is out of any doubt that technological progress realizes a speed in the exchange operations of goods and services it is also true that the *smart contracts*, being IT protocols automatically executing the performances stated in the contract when given conditions, verified through the use of automatic techniques, take place. *Smart contracts* do not enable the parties to use their autonomy in the execution phase of the contract, possibly exercising the right of withdrawal, depriving them of the right of using a discretional interpretation of the contract clauses[30].

The issue of determining the personal identity of the parties and the one of the exact singling out of the correspondence between the will of the contractors, the effects arising from the clauses in the contract and the compliance of the limits and the obligations stated by the legal system is still uncertain.

In such a context the intervention of a qualified intermediary is appropriate, and therefore that could also be the Notary, who not only performs the function of a certifying agent but also the one of examining the will of the parties and the one of suggesting in order to adjust it to better realise the ultimate goal the contractors want to pursuit[31].

Those functions in fact, as those aimed at verifying the identity of the parties and their capacity of acting, will barely be implemented in an IT programme due to which there will always be an exposed area for which maintaining the control of man upon technology is desirable.

[27] G. Sartor, 'Gli agenti software: nuovi soggetti del cyberdiritto?' (2002) Contratto e impresa 466; Rinaldi (n. 5) 344.

[28] *Sma*rt *Contracts:* Legal *Framework and Proposed Guidelines for Lawmakers* (5 November 2018) Clifford-Chance <www.ebrd.com/documents/legal-reform/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf?blobnocache=true>.

[29] Rinaldi (n. 5) 345.

[30] See Signori (n. 14) 429 ff.

[31] Ibid., 431, recalling the example given by M. D'Orazi Flavoni, 'La funzione sociale del Notaio' 1954 Rivista del notariato 405.

BLOCKCHAIN APPLICATIONS AND COMPANY LAW

FLORIAN MÖSLEIN

SUMMARY: 1. Introduction. – 2. Technical basics. – 2.1. Distributed cash books as an architecture of trust. – 2.2. Self-enforcing agreements per source code. – 3. Potential for use in company law practice. – 3.1. Identification mechanism. – 3.2. Enforcement tool. – 3.3. Organizational infrastructure.

1. *Introduction*

Blockchain applications begin to transform both companies and company law. At Member State level, for example, the German government has recently commissioned a study to examine the suitability and need for reform of company law in view of blockchain applications.[1] The European Commission also takes a close look at the intersection of blockchain and company law, and is currently considering "additional company law measures to facilitate cross-border expansion and scale-up by SMEs".[2] At the same time, the High-Level Forum on Capital Markets Union is discussing company law measures to make internal company processes more efficient with the help of distributed ledger technologies.[3] Digitalization is likely to trigger further reform steps under company law, and blockchain and distributed ledger technologies represent fundamental challenges for this field of law.[4] The present chapter therefore tries to shed some light on the intersection of blockchain and corporate law. A brief explanation of the technology (below, sub 2) lays the ground for measuring the potential for its use in company law practice (sub 3).

2. *Technical basics*

2.1. *Distributed cash books as an architecture of trust*

The blockchain can be imagined as a decentralized database in which entries are grouped in chronologically sorted, linked blocks.[5] The individual processes are

[1] Cf. Blockchain strategy, adopted by the German Government on 18 September 2019 <https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2019-09-18-Blockchain.html>. For a detailed discussion of the relevant company law questions, see F. Möslein, S. Omlor and N. Urbach, 'Grundfragen eines Blockchain-Kapitalgesellschaftsrechts' (2020) Zeitschrift für Wirtschaftsrecht, in print.

[2] European Commission, An SME Strategy for a sustainable and digital Europe, COM (2020) 103 final, 10 March 2020, 9.

[3] General information on the main activities of this forum can be found at <https://ec.europa.eu/info/publications/cmu-high-level-forum_en>.

[4] U. R. Rodrigues, 'Law and the Blockchain' (2019) 104 Iowa Law Review 679, 728; on the term also M. Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2019) 22; see also P. De Filippi and A. Wright, *Blockchain and the Law* (Harvard University Press 2019) 136; Ph. Hacker and Ch. Thomale, 'The Crypto-Security' in Ph. Hacker, I. Lianos, G. Dimitropoulos and S. Eich (eds), *Regulating Blockchain* (Oxford University Press 2019) 229, 233 ff.

[5] M. Walport, 'Distributed Ledger Technology: beyond block chain - A report by the UK Government Chief Scientific Adviser' (December 2015) 17

represented transparently and unchangeably in these blocks. This creates an electronic register for digital data records, events and transactions, whose administration is not the responsibility of a central office, but is shared by all participants in the distributed computer network.[6] Distributed ledger technologies generally enable the establishment of systems that function reliably without central control authority, even if the participants do not know or trust each other. Their distributed ledgers form a common trust architecture that is independent of intermediaries.[7]

Consensus mechanisms which exclude unauthorized changes using cryptographic procedures ensure uniformity and protection against forgery. For this purpose, a kind of user fee prevents abusive transactions, either in the form of computing effort for solving specific tasks (so-called *proof of work*) or in the form of capital expenditure through the use of cryptographic currencies (so-called *proof of stake*).[8] Differences also exist with regard to accessibility: While so-called open or public blockchains basically grant free access, in so-called private or permissioned blockchains only selected participants are granted the authority to initiate transactions, validate transactions and create new blocks.[9]

2.2. *Self-enforcing agreements per source code*

Rules and sanctions can also be mapped or automatically enforced on the technical basis of the blockchain. Similar possibilities exist with mechanical constructions as well, for example conventional vending machines which only dispense goods after the purchase price has been paid.[10] On the basis of blockchain technologies, however, much more complex rules and enforcement mechanisms can be implemented, moreover in a decentralized, location-independent form and with an integrated processing system: The technology makes it possible to formulate conditions for the execution of transactions, monitor their execution and enforce conditions that the parties involved have previously agreed on.[11] Such self-enforcing agreements, which are depicted in the source code of the blockchain, are called Smart Contracts.[12] They promise to change the economy more than any other feature of the blockchain.[13]

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>.

[6] J. Condos, W. H. Sorrell and S. L. Donegan, Blockchain Technology: Opportunities and Risks, 15 January 2016, 6 ff. <https://sos.vermont.gov/media/253f2tpu/vermontstudycommittee_blockchaintechnology_opportunitiesandrisks_finalreport_2016.pdf>.

[7] In this vein K. Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press 2018).

[8] See, for instance I. Lianos, 'Blockchain Competition. Gaining Competitive Advantage in the Digital Economy', in Ph. Hacker, I. Lianos, G. Dimitropoulos and S. Eich (eds), *Regulating Blockchain* (OUP 2019) 329, 335.

[9] Ibid, 334 ff.

[10] M. Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly and Associates 2015) 16.

[11] Th. Kuntz, 'Konsens statt Recht?' (2020) 220 Archiv der civilistischen Praxis 51, 65.

[12] In more detail, for instance: R. Unsworth, 'Smart Contract This! An Assessment of the Contractual Landscape and the Herculean Challenges it Currently Presents for "Self-executing" Contracts' in Marcelo Corrales, M. Fenwick and H. Haapio (eds), *Legal Tech, Smart Contracts and Blockchain* (Springer 2019) 17; B. Carron and V. Botteron, 'How Smart Can a Contract be?', in D. Kraus, Th. Obrist and O. Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Elgar 2019) 101.

[13] 'Disrupting the Trust Business' (15 July 2017) The Economist <https://www.economist.com/the-world-if/2017/07/15/disrupting-the-trust-business>.

However, the term coined by *Nick Szabo* in the 1990s is hard to grasp.[14] It is misleading because Smart Contracts do not necessarily qualify as contracts in the legal sense. They trigger technical, but not necessarily legally effective changes.[15] However, they can control, monitor and document legally relevant actions due to two characteristic features: Smart Contracts can map agreed rules and sanctions technically, and they can implement them automatically.[16] In this respect, they serve as a functional equivalent to legal contracts that promises reliable enforcement, but opens up little scope for evaluation due to greater formalization.[17] Because of this functionality, the blockchain is called "regulatory technology", i.e. a technology "that can be used both to *define* and *incorporate* legal provisions into code, and to enforce them".[18]

3. *Potential for use in company law practice*

Applications of blockchain and distributed ledger technologies are discussed in various areas of law, in particular in securities regulation with respect to initial coin offers, security tokens and digital bonds.[19] In contrast, the company law discussion is still in the starting blocks, but is increasingly triggered by the above-mentioned legal policy initiatives.[20] In company law practice, three levels of increasing use of these technologies can be distinguished, namely the identification of shareholders, the enforcement of company law obligations, and the establishment of independent organizational infrastructures.

3.1. *Identification mechanism*

As a decentralized, transparent database, the blockchain promises the simple, unambiguous identification of shareholders. The importance of such identification, especially for listed companies with cross-border shareholders, has recently been emphasized by the second EU Shareholder Rights Directive.[21] The exercise of shareholders' rights,

[14] N. Szabo himself uses different definitions in 'Smart Contracts' (1994) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>, and 'Smart Contracts: Building Blocks for Digital Markets' (1996) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html>.

[15] They are binding in a factual sense, though, cf. S. Breidenbach and F. Glatz (eds), *Rechtshandbuch Legal Tech* (C.H. Beck 2018), 112 (5.3, para. 12).

[16] In detail F. Möslein, 'Smart Contracts im Zivil- und Handelsrecht' (2019) 183 Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht 254, 264-266; cf. also id in T. H. Braegelmann and M. Kaulartz (eds), *Rechtshandbuch Smart Contracts* (C.H. Beck 2019), paras 23-28.

[17] See again Möslein (n 16), 269.

[18] P. de Filippi and S. Hassan, 'Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code' (5 December 2016) First Monday 21 <http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657>.

[19] Cf. for example on these questions Ph. Hacker and Ch. Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' (2018) 15 European Company and Financial Law Review 645.

[20] See above (n 1 to 3).

[21] Cf. recital 4 of the Directive (EU) 2017/828 of the European Parliament and of the Council of 17 May 2017 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement, OJ EU No. L 2017/132, 1 ("prerequisite to direct communication between the shareholders and the company and therefore essential to facilitating the exercise of shareholder rights and shareholder engagement").

such as voting, information or legal action rights, as well as the enforcement of claims under company law require the clear identification of the respective entitled or obligated claimant or opponent. The prevailing custody practice, however, makes this identification difficult because shares are typically not held directly, but through a chain of intermediaries.[22] The Directive therefore operates with cascade-like information obligations. For example, the German implementation in Section 67d (1) of the German Stock Corporation Act (AktG) states that the listed company may require an intermediary holding shares in the company to provide information on the identity of the shareholders and on the next intermediary. The more ramified and multi-layered the custody trees, however, the more complex, costly and error-prone the intermediary-based identification becomes. The IT systems of issuers and intermediaries are so complex to adapt that the German legislator even felt compelled to postpone the start of application of the relevant provisions, despite the expiry of the implementation period.[23]

As a decentralized, transparent database, the blockchain has the potential to reduce these difficulties: If shareholders are listed in such a database and if shareholder changes are also reliably represented by adding new blocks, the requirement "to know your shareholder" is much easier to meet.[24] It only takes a look into the database. Shares are immediately traceable.[25] Online platforms offer such technical solutions for the purposes of exercising and representing voting rights.[26] Beyond doubt, this alternative form of shareholder identification also raises questions of technical design. On the one hand, the register must be kept in a legally permissible form. The provision on the share register in Section 67 of the German Stock Corporation Act (AktG) raises the question of whether the decentralization typical of blockchains is permissible.[27] Even if para. 67 (3) AktG provides that deletion and new entry are made upon notification and proof, it is recognized that the management board does not need to operate the register itself, but that the provision and monitoring of the technical framework are sufficient.[28]

[22] In more detail D. Zetzsche, 'Aktionärsidentifikation, Aktionärslegitimation und das Hauptversammlungsverfahren nach ARUG II' (2020) Aktiengesellschaft (Die) 1, 3.

[23] Accordingly, the provision also of Section 67d AktG shall be applied for the first time to General Meetings that are convened after 3 September 2020, according to Art. 26j (4) EGAktG.

[24] See in particular U. Noack, 'Identifikation der Aktionäre, neue Rolle der Intermediäre – zur Umsetzung der Aktionärsrechte-Richtlinie II' (2017) Neue Zeitschrift für Gesellschaftsrecht 561, 561 ff.; D. Zetzsche, 'Know Your Shareholder, der intermediärsgestützte Aktionärsbegriff und das Hauptversammlungsverfahren' (2019) Zeitschrift für Unternehmens- und Gesellschaftsrecht 1.

[25] G. S. Geis, 'Traceable Shares and Corporate Law' (2018) 113 Northwestern University Law Review 227 ("poised to allow for specific share identification and precise records of share provenance"); similar De Filippi and Wright (n 4), 134.

[26] The electronic trading platform Nasdaq, for example, offers a corresponding e-voting application (but for the time being only in South Africa, within the EU only pilot tests in Estonia), see <https://www.nasdaq.com/solutions/evoting-technology>. Within Citigroup, the *Proximity* platform was developed for the purpose of proxy voting, see <https://www.citivelocity.com/proxymity/>. For further examples, see M. van Rijmenam, 'How Blockchain Proxy-Voting Will Improve Shareholder Engagement' (4 October 2019) Datafloq <https://datafloq.com/read/blockchain-proxy-voting-improve-shareholders/6977>; Ch. van der Elst and A. Lafarre, 'Blockchain and smart contracting for the shareholder community' (2019) 30 European Business Organization Law Review 111, 130 ff.

[27] M. Beurskens, 'Blockhain und Gesellschaftsrecht' in A. Bergmann, M. Hoffmann-Becking and U. Noack (eds), *Recht und Gesetz - Festschrift for Ulrich Seibert* (Verlag Dr. Otto Schmidt 2019) 71, 80.

[28] U. Hüffer and J. Koch (eds), *Kommentar zum Aktiengesetz* (14th ed., C.H. Beck 2020), para. 67(5) AktG,.

Decentralized register maintenance should therefore also be permissible, but only in the technical form of the permissioned blockchain in which only selected participants authorized by the board of directors can validate transactions. On the other hand, secrecy requirements must be taken into account. Such requirements are partly rooted in the interests of the participants, but they can also be legally prescribed.[29] Secrecy is technically possible because the transparency of the blockchain can be limited and users generally appear by public key, so that pseudonymity prevails anyway.[30] Technical designs that meet these requirements are therefore possible. They do not reduce the efficiency advantages that blockchain identification promises compared to intermediary-based shareholder identification.[31] Even if this technical device is limited to the mere function of data recording, it already has far-reaching significance for corporate law: "It will change the structure of shareholder lawsuits, alter the allocation of corporate governance rights, and require lawmakers to rethink fundamental principles of shareholder responsibility for corporate misdeeds".[32]

3.2. *Enforcement tool*

The blockchain can also be used to automatically enforce rules and sanctions. As is well known, corporate governance consists of norms that determine the organization and in particular the decision-making of a company. These norms root both in company law and in the articles of association, but they are supplemented by economic and other incentives, customs and recommendations.[33] They define the rights and duties of corporate actors, in particular of management and shareholders. They set preventive behavioral incentives, but they also require effective enforcement mechanisms in case of conflict.

The blockchain provides the possibility of mapping those rules in technical code and thus automates their enforcement.[34] A common example are security tokens which represent property rights and, with the help of Smart Contracts, automatically trigger interest or dividend payments when certain parameters occur (e.g. distribution resolution).[35] The possible applications of such technical devices are not limited to property rights, but extend to the entire organizational structure under company law.[36] In particular, internal company decision-making processes can be automated.[37] For example, companies can use the software from *Boardroom* to organize decision-making in the boardroom.[38] With the recent introduction of virtual general meetings, the application

[29] Cf. for example the limits of the possibilities of inspection laid down in para. 67(5) sentence 1 German AktG; in more detail Beurskens (n 27), 81.

[30] On the pseudonymity of the Blockchain in general De Filippi and Wright (n 4), 38 ff.

[31] van der Elst and Lafarre (n 26), 133; see also F. Panisi, R. P. Buckley and D. Arner, 'Blockchain and Public Companies: A Revolution in Share Ownership Transparency, Proxy-Voting and Corporate Governance?' (2019) 2 Stanford Journal of Blockchain Law & Policy 189.

[32] Geis (n 25).

[33] Generally, on mechanisms of *private ordering* M. A. Eisenberg, 'Private Ordering Through Negotiation: Dispute -Settlement and Rulemaking' (1976) 86 Harvard Law Review 637.

[34] In the same vein De Filippi and Wright (n 4), 133: "With a blockchain, organizations could decide to use code to implement parts of the organization's rules and procedures".

[35] See, for instance, Hacker and Thomale (n 19), 650.

[36] In detail De Filippi and Wright (n 4), 133-136.

[37] Beurskens (n 27), 89 ff.; G. Spindler, 'Gesellschaftsrecht und Digitalisierung' (2018) Zeitschrift für Unternehmens- und Gesellschaftsrecht 17, 50.

[38] See <www.boardroom.to>; see De Filippi and Wright (n 4), 135; see also L. Enriques and D. A

possibilities also extend to respective resolutions. Applications such as *Otonomos* offer the possibility of using blockchain-based governance structures within the framework of applicable corporate laws: "Using Otonomos, people can form a corporation [...] that is entirely administered through a blockchain, including procedures related to voting, dividends, and capital increases".[39]

3.3. *Organizational infrastructure*

In a third step, blockchain technology can be used to not only enforce regulations, but to replace them with technical code. As a *regulatory technology,* it enables organizational structures even detached from the structures of company law: It allows the creation of "companies which consist only of computer code".[40] The technology thus promises an alternative to law as an infrastructure of human cooperation.[41] Platforms such as *Aragon* ("Unstoppable organizations: Aragon provides all the necessary tools for human collaboration") offer corresponding forms of organizations.[42] These forms are usually called "Decentralized Autonomous Organizations" (DAOs), and they are enjoying increasing popularity.[43]

Smart Contracts serve as the building blocks of such a DAO. They allow the incorporation of even complex rules. Smart Contracts can be made dependent on external events (such as stock market prices or turnover figures) by using so-called "oracles" as an interface to reality to check the occurrence of conditions.[44] Individual clauses are stored[45] as decentralized applications (DApps) on platforms such as *Ethereum* and can be combined as in a modular system.[46] For situations where their rules turn out to be incomplete and disputes arise, the platforms offer their own dispute resolution mechanisms ("the world's first digital jurisdiction").[47]

These building elements enable architectures in which company-like organizations

Zetzsche, 'Corporate Technologies and the Tech Nirvana Fallacy' (2020) 71 Hastings Law Journal, forthcoming (Working Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3392321>.

[39] De Filippi and Wright (n 4), 135; for more details see <https://otonomos.com/>; there are, for example, corporate forms available in Switzerland (GmbH), the United Kingdom (LLP), Delaware (LLC and C-Corp.), Hong Kong (Ltd.) and Singapore (Pte. Ltd.).

[40] This is the formulation of the founder of Slock.it, Ch. Jentzsch, in his TedX Talk of 'The Company Which Consists Only of Computer Code' (9 January 2017) <https://www.youtube.com/watch?v=EJrPW3254wg>.

[41] On private law as an infrastructure see, for instance, K. Riesenhuber and F. Möslein, 'Contract Governance - A Draft Research Agenda' (2009) 5 European Review of Contract Law 248, 269.

[42] Cf. <https://aragon.org>.

[43] See, for instance, Hacker and Thomale (n 4), 233 ff.; I. Lianos, 'Blockchain Competition. Gaining Competitive Advantage in the Digital Economy: Competition Law Implications', in Ph. Hacker, I. Lianos, G. Dimitropoulos and S. Eich (eds), *Regulating Blockchain* (Oxford University Press 2019) 329, 347 ff.; more extensively B. Mienert, 'Blockchain-basierte dezentrale autonome Organisationen und Gesellschaftsrecht' (Diss. Marburg 2020), forthcoming.

[44] De Filippi and Wright (n 4), 75.

[45] See U. R. Rodrigues, 'Law and the Blockchain' (2018) 104 Iowa Law Review 679, 698 ff.; cf. also the numerous "building instructions", for example <https://codeburst.io/build-your-first-ethereum-smart-contract-with-solidity-tutorial-94171d6b1c4b>.

[46] In detail D. Tapscott and A. Tapscott, *The Blockchain Revolution* (Penguin 2016), 117-122.

[47] Cf. <https://aragon.org/network/>; in more detail F. Möslein, 'Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions' in Ph. Hacker, I. Lianos, G. Dimitropoulos and S. Eich (eds), *Regulating Blockchain* (Oxford University Press 2019) 275, 276 ff.

can be easily established. DAOs promise some advantages over law-based companies:[48] First, their establishment is cheap and simple. Secondly, there is far greater freedom of organizational design than in most national company laws, especially in German stock corporation law which is almost entirely mandatory (see para. 23(5) AktG). Thirdly, the regulatory offerings are not bound to national legal systems, but claim global reach. Fourthly, the blockchain-based enforcement mechanisms are simple and effective. On the other hand, however, the addressees should not underestimate the disadvantages that exist in comparison to traditional company law: Firstly, there is still a lack of practical experience or the experiences are deterrent (e.g. the 50 million US$ hack of the notorious "The DAO").[49] Secondly, technology-based rules function automatically, but also very mechanically. They lack the scope for interpretation and discretion that would enable fair results in individual cases if legal rules were applied.[50] Thirdly, the prospect of legal protection is uncertain because DAOs are conceived as a deliberate departure from the law and the admissibility of corresponding legal remedies is still unclear. Fourthly, this legal uncertainty weighs particularly heavily on third parties who, unlike the shareholders, do not consciously opt for the digital ecosystem of the blockchain. Lenders, suppliers or employees will often not be prepared to provide services to entities against which they may not be able to sue counterclaims. As long as it is not clear whether DAOs can offer the privilege of limited liability, these forms of organizations are not very attractive for company founders either.

Accordingly, there is a tendency to combine the respective advantages of blockchain and company law instead of treating these technical and legal infrastructures as exclusive alternatives. On the one hand, first platforms offer legally compliant DAOs – so-called LAOs – in which the liability of the shareholders is limited in a legally secure manner. For this purpose, conventional companies are included as so-called "limited liability wrappers".[51] Even if these wrappers are of US-American origin, LAOs enjoy the freedom of establishment in Europe: In combination with Art. XXV para. 5 sentence 2 of the German-American Commercial Treaty, LAOs enjoy the same legal recognition in Germany as in the USA.[52] On the other hand, first jurisdictions are designing

[48] See again <https://aragon.org/> ("Global by default", "fast and easy" and "truly sovereign"); also 'An Operating System for Collective Intelligence' (22 April 2018) DAOstack 5, <https://daostack.io/wp/DAOstack-White-Paper-en.pdf>; moreover W. A. Kaal, 'Blockchain-based Corporate Governance' (2021) 4 Stanford Journal of Blockchain Law & Policy, forthcoming.

[49] In detail, for instance, F. Coppola, 'Ethereum's DAO Hacking Shows That Coders Are Not Infallible' (20 June 2016) Forbes <https://www.forbes.com/sites/francescoppola/2016/06/20/the-dao-hacking-shows-that-coders-are-not-infallible/>.

[50] Similar, with a view to Smart Contracts, Möslein (n 16), 289; see also K. Werbach, 'Trust, But Verify: Why the Blockchain Needs the Law' (2018) 33 Berkeley Technology Law Journal 489 ("Trust, But Verify: Why the Blockchain Needs the Law").

[51] 'The Era of Legally Compliant DAOs' (26 June 2019) OpenLaw <https://medium.com/@OpenLawOfficial/the-era-of-legally-compliant-daos-491edf88fed0>; see also 'A Taxonomy for LAOs: Making Sense of the Emerging LAO Ecosystem' (13 November 2019) Medium <https://medium.com/@thelaoofficial/a-taxonomy-for-laos-making-sense-of-the-emerging-lao-ecosystem-1122b035fe1a>.

[52] Entscheidungen des Bundesgerichtshofes in Zivilsachen (BGHZ) 154, 185, in accordance with Court of Justice of the EU, Case C-208/00, *Überseering*, judgment of 5 November 2002; specifically on the recognition of regulated DAOs (from a Swiss perspective) S. Riva, 'Decentralized Autonomous Organisations as subjects of law' (Master Thesis, University of Neuchâtel 2019) 36 ff. <https://libra.unine.ch/Publications/40515>.

legal forms that are specifically tailored to DAOs or are at least suitable for their establishment.[53] In the long run, these developments are likely to amount to a cooperation between national company law and the blockchain. It is just not yet clear how this cooperation will be structured in detail.[54]

[53] For example, Malta with Act No. XXXIII of 20 July 2018 (Innovative Technology Arrangements Bill) <https://parlament.mt/media/95214/act-xxxiii-innovative-technology-arrangements-and-services-act.pdf>; for more details, M. Ganado, 'Maltese Technology Foundations' (2018) Working Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3245783>. Similarly, Liechtenstein with the segmented legal entity pursuant to Art 243 ff. PGR; and the US State of Vermont with Blockchain-Based Limited Liability Company pursuant to Vermont Act No. 205 (279), An act relating to blockchain business development.

[54] In the same sense on the relationship between Smart Contracts and contract law, Möslein (n 16), 289 ff.

ANONYMITY AND PSEUDONYMITY.
FINTECH AND THE KEY ISSUE OF TRACEABILITY

ELISABETTA PEDERZINI

SUMMARY: 1. Introduction. – 2. Cryptocurrencies, anti-money laundering, financing of terrorism: criminal profiles of traceability. – 3. Fintech, European GDPR and personal data processing: Private profiles of traceability.

1. *Introduction*

In general terms, the theme of traceability evokes at least two distinct meanings or spheres of meaning. From an objective point of view, it addresses the possibility of finding over time, in a stable, lasting, and freely accessible manner, intelligible signs that give certainty to the occurrence of a pre-existing fact, situation, or condition. On a subjective level, instead, the concept of traceability suggests the ability to report a fact, act, situation, or condition unequivocally to one and only one person, who is clearly identified or easily identifiable. In each case, the notion of traceability is understood to be entirely independent of the legitimacy of the fact, act, or situation in question, and the legal imputability of the act to the identified person. Traceability concerns, as it were, a verification of effectiveness and does not involve, directly or automatically, a judgment that can only be made subsequently and that pertains not to the traceable path itself but rather to the object to which the path refers and/or the relationship between the object and the person to which it refers.

Traceability therefore concerns sets of information, both objective and subjective in nature, related to the factors of time and space.

With respect to this theme, crucial questions exist, both of a purely private nature and related to straightforward criminal law issues: on the one hand, the comparison with the protection and processing of personal data in compliance with Regulation (EU) 2016/679 (*General Data Protection Regulation – GDPR)* and, on the other, the possible violation of the rules designed to prevent the use of the financial system for the purpose of money laundering and criminal financing of terrorism.

Acknowledged with immediacy and priority in the overhaul of the system – and in the consequent judgment of compliance with the principles of a given legal system or of contradiction with certain disciplines – is the reference to the technology summarized as *blockchain*, which the *Fintech* universe crosses and underlies in its multiple manifestations, in order to summarily outline its structural characteristics and operating modes.

The *blockchain* is one of the *Distributed Ledger Technologies*, built on a register divided into connected network blocks, so that each transaction must be validated on the basis of a process of distributed consent involving all the nodes (or blocks). The *blockchain* is therefore a shared, decentralized, distributed, non-modifiable, transparent, encrypted database in accordance with the model of asymmetric key cryptography, which continuously, permanently and unalterably records a set of transactions through a *peer-to-peer* network.[1] Among the nearly infinite functionality and application potentials, those which stand out in the financial sector include support for the creation and circulation of virtual currencies and the completion of totally dematerialized agreements, known as *smart contracts*.

Although all *blockchains* are characterized by a distributed and shared architecture, it is possible to use an internal classification that juxtaposes *permissionless* and *permissioned blockchains*.

The *permissionless blockchains* are completely decentralized, in the sense that anyone can freely join the network and every node (user), after logging in, can carry out transactions, validate transactions, or create new blocks on the *network*: Bitcoin and Ethereum (more precisely, the technologies from which the cryptocoins Bitcoin and Ethereum originate) belong to this subset. On the other hand, *permissioned blockchains* have a structure that is only partially decentralized, in the sense that the entry of new nodes that are added to the system must be authorized by "special nodes", and that the process of validating and sending transactions is entrusted only to a select and previously identified group of users or "consortia". Regarding the related but different notion of the transparency of or accessibility to the reading of *blockchain* information, depending on whether the viewing of the transaction log is freely accessible or has controlled access, the distinction may arise between *public* and *private blockchains*.[2]

The adjective that is most frequently associated with *blockchain* technology is *disruptive*: the emphasis of one particular operating characteristic or potential application often leads to resolutely contradictory considerations in terms of risk or threat to the system or beneficial and favorable opportunity.[3] Technology, however, in itself is not "good or bad", as such judgment depends not only on the use made of it, and therefore on the purposes of the men and women making use of it, but also on the perspective from which it is viewed and thus from the purposes implicit in, or underlying, such observation.

2. *Cryptocurrencies, anti-money laundering, financing of terrorism: criminal profiles of traceability*

The enormous potential offered by the tracing of financial transactions exists in the prevention and repression of criminal phenomena: the impossibility or the extreme

[1] M. Cavallo and M. Lillà Montagnani, 'L'industria finanziaria tra Fintech e Techfin: prime riflessioni su Blockchain e Smart Contract', in G. Finocchiaro and V. Falce (eds.), *Fintech: diritti, concorrenza, regole* (Bologna 2019) 329 ff.; M. L. Perugini, *Distributed ledger technologies e sistemi di blockchain: digital currency, smart contract e altre applicazioni* (Milano 2018); A. M. Antonopoulos, *Mastering bitcoin: programming the open blockchain* (Sebastopol 2017); M. Bellezza, 'Blockchain'*,* in M. T. Paracampo (eds.), *Fintech* (Torino 2017) 217 ff.; M. Giuliano, 'La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio' (2018) Diritto dell'informazione e dell'informatica 997; M. Swan, *Blockchain, Blueprint for a New Economy* (Sebastopol 2015); A. Wright and P. De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664>.

[2] See L. Piatti, *Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto,* in *Ciberspazio e diritto* (Modena 2018) 182 ff.; Giuliano (n. 1), 1004 ff.

[3] D. A. Zetsche, R. P. Buckley and D. W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) 14 EBI – Working Paper Series <https://ssrn.com/abstract=3018214>; D. Tapscott and A. Tapscott, *Blockchain revolution* (London 2016).

difficulty of identifying and reconstructing financial movements and the negotiations of values, and of retracing the steps backwards until they can be unequivocally linked to one or more specific persons, constitutes the ground on which crimes such as tax evasion, corruption, illegal trafficking of arms or drugs, and, above all, the laundering of money of illegal origins and the secret financing of terrorist activities, can take root. The very stability of the financial system as a whole is seriously threatened, if not fatally compromised, by the harmful consequences for the sectors and operators that move within the cornerstones of legality.

Financial institutions, both in Europe and internationally, have for some time been clearly aware of the problem and stress the urgency of regulatory intervention.[4]

With specific regard to the European Union, a Fifth Anti-Money Laundering Directive was recently approved as a compendium and modification of previous harmonization measures, as a clear demonstration of the heightened attention paid to a sector crucial for the implementation of the single market and considered to render it particularly vulnerable.[5]

A common and constitutive element, at least of the main criminal cases, which consolidate their operating dynamics on the lack of transparency, both objective and subjective, is the use of particular digital instruments representative of value and susceptible of being the object of exchange, those identified as cryptocurrencies or virtual currencies, starting with the famous bitcoins and eventually joined by others such as ethereum, litecoin, titcoin, peercoin, monero, ripple, zcash, and the list goes on.[6]

[4] See the documents drawn up respectively by the FATF - Financial Action Task Force (the *Virtual Currencies: Key Definitions and Potential AML/CTF Risks* - FATF 2014 report and the subsequent guidelines *Guidance for a Risk-Based Approach to Virtual Currencies*, published for the first time in 2015, then updated in June this year - FATF 2019), by the European Central Bank (a 2012 report subsequently updated as the *Virtual Currency Schemes: a further analysis* - ECB 2015) and finally by the European Banking Authority (*Opinion 2015/08 on Virtual Currencies* - EBA 2014). Among the greater than seventy risks subject to survey and divided into categories (such as Risks for users, Risks not dependent on participants in transactions, Risks related to system integrity, Risks related to currency exchange in *Fiat Coins*, Risks for Regulatory Authorities), the category denoting *Risks linked to system integrity* – all such considered by the EBA to be "high" – concern in particular: laundering of the proceeds of crime through the deposit and transfer of cryptocurrencies in a rapid, anonymous, and irrevocable manner at a global level; concealment of the criminal origin of funds and the consequent obstacles to recovery, seizure and confiscation; use for the purpose of financing terrorism; anonymous extortion; facilitation of engaging people in criminal activities.

[5] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and (EU) 2013/36. The other four European Directives on anti-money laundering and counter-terrorist financing followed one after another from 1991 to 2015, always preceded by the Recommendations of the FATF - Financial Action Task Force or FATF - Group on International Financial Action, established in 1989 at the OECD. The urgency of the revision of the Fourth Anti-Money Laundering Directive (Directive (EU) 2015/849) is in relation to the sequel of terrorist attacks of Islamist origin that have devastated Europe since the Paris massacre and with the affair known as *Panama Papers*.

[6] The literature on *cryptoassets* and *cryptocurrencies* is already extensive. See, among others: M. Mancini, *Valute Virtuali e Bitcoin*, in *AGE*, 2015; S. Capaccioli, *Criptovalute e bitcoin*: *un'analisi giuridica* (Milano 2015); B. Kelly, *The Bitcoin Big bang: How Alternative Currencies Are About to Change the World* (New Jersey 2015); M. Amato and L. Fantacci, *Per un pugno di Bitcoin* (Milano 2016); M. Mancini, 'Bitcoin: rischi e difficoltà normative' (2016) Banca impresa 127; H. Halaburda and M. Sarvary, *Beyond Bitcoin: the Economics of Digital Currencies* (New York 2016); A. M. Antonopoulos, *Mastering bitcoin:*

There is no universally accepted and unequivocal definition of cryptocurrency. However, we may consider the following definition of virtual currency which, to a good degree of approximation and commendably all-inclusively, appears in both the Fifth Anti-Money Laundering Directive, having been incorporated as it had been earlier recognized by the European Banking Authority in 2014, and in the Italian legislature's recent amendment of its national anti-money laundering regulations in Italian Legislative Decree No. 125/2019: "a digital representation of value which is not issued or guaranteed by a central bank or public authority, is not necessarily linked to a legal tender currency, does not have the legal *status* of currency valuation or money, but is accepted by natural and legal persons, is used as a medium of exchange for the purchase of goods and services or for investment purposes, and can be transferred, archived and negotiated electronically" (Art. 1, co. 2, let. *qq,* Legislative Decree No. 231/2007).

Note the explicit inclusion of "investment purpose" created precisely as a result of the decree implementing the Fifth Directive: the previous text of the rule – as amended by Legislative Decree No. 90/2017, implementing the Fourth Anti-Money Laundering Directive – in fact referred only to the use as a means of exchange or payment even though the European Banking Authority had already grasped the heterogeneity of its application, not excluding, alongside the purpose of exchange, the holding *for investment purpose*.[7]

Following the classification adopted by the European Central Bank in the aforementioned 2015 Report, a relationship between class and species must be established between virtual currencies and cryptocurrencies since almost all cryptocurrencies fall within the category of *Virtual Currency Schemes with Bidirectional Flow*, characterized by full and perfect convertibility into legal tender (unlike the *Closed Virtual Currency Schemes*, which circulate exclusively within a virtual environment, and the *Virtual Currency Schemes with Unidirectional Flow*, which can be purchased with legal currency but cannot converted to it).[8]

A completely peculiar and, so to speak, paradigmatic remark must be emphasized with respect to the first, and still most widespread, of cryptocurrencies, the bitcoin,

programming the open blockchain (Sebastopol 2017); Paola Liberanome, 'Criptovalute tra anarchia e difficili tentativi di regolamentazione', in F. Fimmanò and G. Falcone (eds.), *Fintech* (Napoli 2019) 419 ff.; C. Pernice, 'Crittovalute e bitcoin: stato dell'arte e questioni ancora aperte', in F. Fimmanò and G. Falcone (eds.), *Fintech* (Napoli 2019) 491 ff.; A. M. Gambino and Ch. Bomprezzi, 'Blockchain e criptovalute', in G. Finocchiaro and V. Falce (eds.), *Fintech: diritti, concorrenza, regole* (Bologna 2019) 267 ff.; M. T. Chimienti, U. Kochanska and A. Pinna, 'Understanding the crypto-asset phenomenon, its risks and measurement issues' (2019) ECB Economic Bulletin; 'ECB Crypto-Assets Task Force, *Crypto-Assets: implications for financial stability, monetary policy, and payments market infrastructures* (ECB 2019).

[7] The Bank of Italy also used the same term in its Communication of 30 January 2015 on virtual currencies. Consistently, the Directive (EU) 2018/843 states: "Although virtual currencies can often be used as a means of payment, they could also be used for other purposes and be used more widely, for example as a means of exchange, of investment, as valuable reserve assets or in an online casino". As is well known, virtual currency or money is as distinct from electronic money as it is from so-called complementary currency: see V. De Stasio, 'Verso un concetto europeo di moneta legale' (2018) Banca, borsa e titoli di credito 747.

[8] See R. Bocchini, 'Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche' (2017) Diritto dell'informazione e dell'informatica 27, 52 ff.

which thus offers apt opportunity to investigate the risks and penal consequences of (non) traceability.[9]

In the international context, the regulations of advanced capitalist countries encompass money laundering and the financing of terrorism – and more generally the circulation of money – in a detailed regulation based on prevention through maximum transparency in financial negotiations, so as to verify with certainty the identity of the parties of all transactions both in a formal sense (who has the funds, and to whom the funds are destined) and in a substantial sense (correspondence with the actual recipients).[10]

Without undervaluing the release from spatial coordinates that makes *Fintech* a plausible "free zone" potentially without geographic boundaries in which to bury vast monetary sums destined for diverse illegal purposes or to facilitate the re-emergence of large sums as immaculate despite coming from the commission of computer or traditional crimes, once again an important distinction is represented by the technical operating characteristics of cryptocurrencies. As indicated above, the use of *blockchain* technology allows, with respect to the operations performed, non-retractability and invariability, accurate time stamping, stability, and indelibility of the registered operations once they have occurred. Conversely, with respect to the identification of the subjects, it creates more or less definitive and irreversible forms of opacity and concealment. The borderless dimension of a globalized world, the instantaneous immediacy of transactions and the inclination toward anonymity thus represent the ideal conditions for the commission of crimes which, due to the structural elusiveness and the impossibility of uniquely attributing the commission to a specific person, are likely to remain dramatically unpunished.

However, the paradigm of subjective traceability connected to the circulation of bitcoins can be qualified not in terms of true and real anonymity, but rather of *pseudonymity*.[11] The non-immediacy of identification, concealed due to the use of an alphanumeric computer code, is in fact surmountable thanks to the use of particular software; with it, the authorities of different countries can crack the pseudonym and reveal the identity of the user who has used it to activate an account, in order to avoid the risk of that user systematically eludes legality, and to allow the imposition of criminal sanctions foreseen by the law.

[9] B. Bandiera, 'Fintech e antiriciclaggio', in M. T. Paracampo (eds.), *Fintech* (Torino 2017) 259 ff.; G. P. Accinni, 'Profili di rilevanza penale delle "criptovalute"' (2018) Archivio penale 1; F. Di Vizio, 'Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. Lo statuto delle valute virtuali. Le discipline e i controlli', in F. Fimmanò and G. Falcone (eds.), *Fintech* (Napoli 2019) 291 ff.; M. Krogh, 'Bitcoin, Blockchain e le transazioni in valute virtuali ed i rischi di riciclaggio. Il ruolo del notaio', in F. Fimmanò and G. Falcone (eds.), *Fintech* (Napoli 2019) 385 ff.

[10] M. Krogh, 'Transazioni in valute virtuali e rischi di riciclaggio, Il ruolo del notaio' (2018) Notariato 155.

[11] M. Möser, R. Böhme and D. Breuker, 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem', in *2013 eCrime Researchers Summit (eCRS 2013)* (IEEE 2014) 76 ff.; E. J. Imwinkelried and J. Luu, 'The Challenge of Bitcoin Pseudo-Anonimity to Computer Forensics' (2016) 52 Criminal Law Bulletin 191; Di Vizio (n. 9), 304 ff.: "Bitcoin uses public key cryptography, an asymmetric cryptographic algorithm that uses two mathematically generated keys: the private key, which is used to 'encrypt' or digitally sign the document, the 'digital money', and the public key, which is used to 'decrypt' the message or verify the signature".

The complete transparency of all registered operations makes it possible to uniquely attribute each transaction to the public key associated with it: if the accessible certainty always concerns the starting *account*, the receiving *account* and the amounts individually negotiated between the one and the other, the technological unveiling process makes it possible to trace the private key and therefore the real identity of the individuals that have used, exchanged or circulated the bitcoins on the *blockchain*.

The possible secondary and selective traceability of the pseudonymity, due to technological precautions, however, borders on the most insurmountable *anonymity* due to the application of other technological tools that conceal and irreversibly mask the real identity of the users/contractors within the dynamics of the blockchain.[12]

In the Bitcoin system anyone can obtain a pair of keys, public and private, to transfer cryptocurrency without any need for prior identification, and the number of public keys generated and capable of being generated by the system is potentially infinite: to each personal identity, however masked, there can be associated as many public keys – and as many private – as are the transactions made, easily breaking the correspondence between the user-conferrer or user-recipient and the sum of registered operations, which can no longer be connected even to a single *account*.[13] Software systems, increasingly available on the market, carry out so-called *mixing* or *tumbler* services, i.e. the mixing between the accounts of origin and destination, so that the individual financial movements and the payments made are randomly scattered like a deck of cards on a gaming table, preventing the precise reconstruction of the chronological chain, and the aggregation and symmetry between registrations.[14]

The primeval bitcoins have gradually been joined by other cryptocurrencies, with a generically summarized expression referred to as *Alternative Coins* or Altcoins, some of which are able to guarantee an almost inaccessible level of anonymity thanks to different operating algorithms.[15] Two such examples are *Monero*, released on the market in 2014 and characterized by the correspondence of a different pair of keys for each individual operation and automatically governed by a *mixing* system, and *ZCash*, launched in 2016, which allows users to hide the transactions made, the recipients, and the related amounts.[16] At the state of the art, nothing seems to prevent, however, criminals themselves from electing to generate their own cryptocurrency with which to indiscriminately handle or exchange vast sums, and cleanse the proceeds deriving from all forms of illegal activity.

In this context, in which the technological environment seems to shun any pretense of standardization, the reactions of regulators attest to the limits of the real world (and those of the economy), intervening at the moment and at the time of the conversion of the virtual currency into currency having legal tender. As put forth in Recital 8 of the

[12] Accinni (n. 9) 5.

[13] M. Martoni, 'Documento informatico e firme elettroniche', in C. Di Cocco and G. Sartor (eds.), *Temi di diritto dell'informatica* (Torino, 2017) 27 ff.

[14] Multiple *mixing service* systems exist with evocative names such as Bitcoin Laundry, Bitcoin Fog, Bitlaunder, Cleanbit, Safewallet, Darkbit, Easycoin, etc.

[15] At the time of writing, almost 2,500 cryptocurrencies have been identified, in fact, as "alternatives" to bitcoin, although the latter continues to account for over 60% of the total market <www.coinmarket.cap>.

[16] L. D'Agostino, 'Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017' (2018) Rivista di diritto bancario 12.

preamble of the aforementioned Fifth Anti-Money Laundering Directive, in order to combat money laundering and financing of international terrorism, the competent authorities of the EU member countries must be able to monitor the use of virtual currencies through constant control over a plurality of subjects through stringent information and verification obligations. Therefore, there is emphasis on the "fundamental importance" of expanding the scope of the previous Fourth Directive (Directive (EU) 2015/849) to include service providers whose activity consists in the exchange between virtual currencies and currencies with legal tender status – namely coins and banknotes considered to be legal tender and electronic money when accepted as a medium of exchange in the issuing country - and digital wallet service providers[17].

Along the same lines, even before the deadline for implementation set at 10 January 2020, but already at the time of the transposition of the aforementioned and amended Fourth Directive, the first of all European regulators to act was the Italian legislature. In fact the Legislative Decree No. 90 of 25 May 2017, reformed the Legislative Decree No. 231 of 21 November 2007, containing the internal regulations concerning the prevention of the use of the financial system for the purpose of money laundering and the financing of terrorism, by extending the set of preventive measures aimed at avoiding the mechanism for concealing financial traceability, when implemented by means of virtual digital currency, to *virtual currency exchangers*, i.e. professional operators who, by converting the cryptocurrency into legal tender and legal currency into cryptocurrency, act as access and exit "doors" and are therefore able to identify the people entering and leaving the digital system (Art. 1, co. 2, letter *ff*, and Art. 3, co. 5, letter *i*, Decree No. 231/2007). In particular, the reform extended to these digital money changers the obligations of adequate customer verification (identification of the customer and verification of his/her identity, identification of the effective owner of the funds and his/her identity, acquisition and evaluation of information on the purpose and nature of the ongoing relationship or professional performance, constant monitoring of the relationship with the customer) and the obligation to report to the FIU (Financial Intelligence Unit) any transactions considered suspicious due to their characteristics, the entities involved, the nature, or the connection or division of such, also taking into account the economic capacity and activity carried out by the person to whom they refer (in addition to the obligations to retain data and information collected through systems suitable for ensuring compliance with the rules dictated by the Code regarding the protection and processing of personal data).[18] The implementation of the Fifth Directive represented the opportunity to explicitly extend the anti-money laundering transparency obligations further, to *e-wallet providers*, managers for users of digital wallets, electronic accounts in which the virtual currency is protected by cryptographic keys and in which the virtual currency can be used for transactions, purchases, remittances, and conversions with other users, with recording of all operations and the furnishing of a balance. According to the reformed Articles 1, co. 2, let. *ff-bis*, and 3, co. 5, let. *i-bis*, of the Decree No. 231/2007, the obligations of adequate verification, registration and reporting are now also incumbent on "every

[17] See (n. 6).

[18] Accinni (n. 9) 19; M. Passaretta, 'La nuova disciplina antiriciclaggio: tra sistemi di pagamento innovativi e nuove forme di finanziamento alle imprese', in F. Fimmanò and G. Falcone (eds.), *Fintech* (Napoli 2019) 470 ff.; Pernice (n. 6), 528 ff.

natural or legal person who provides to third parties, on a professional basis, even *online*, services for safeguarding private cryptographic keys on behalf of their customers, in order to hold, store and transfer virtual currency" (digital wallet service providers).[19]

The insufficiency of the safeguards thus created does not however escape the European regulator itself. Recital 9 of the Fifth Directive, in fact, reads: "The anonymity of virtual currencies allows their potential misuse for criminal purposes. The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers. To combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed".

As they intercept and affect only the exit and re-entry into the real world (from the virtual world) by controlling the gatekeeping, this 'toll gate' reveals its inadequacy to regulate the phenomenon in its authentically virtual dimension which is inextricably related to technological evolution.[20]

Alongside the possibility of not allowing the wealth accumulated through the criminal activities to re-emerge in the form of legal currency (which is all the more plausible in conjunction with the widespread acceptance of the cryptocurrency as a means of payment and also with its proven ability to form the object of investment and a reserve amount), and the possibility of converting and re-issuing funds without the use of digital money changers (facilitated precisely by the constant development of technology and the consequent effect of progressive disintermediation at all levels), it is not clear what instruments the national financial information units should equip themselves with in order to associate the addresses of the virtual currency with the identity of the real owner, as called for by European legislation. Nor do technologies or systems capable of linking the certain identity of an individual user to a digital account seem currently available to or from which amounts expressed in bitcoins or other

[19] Before the entry into force of Legislative Decree No. 125/2019, it was unquestionable that they were included among the subjects that provide "third parties, on a professional basis, services functional to the use, exchange and storage of virtual currency" pursuant to Art. 1, par. 2, letter *ff)* of Legislative Decree No. 231/2007. Without prejudice to the obligation to register in a special section of the OAM registry, established pursuant to Art. 128-*undecies* of the Consolidated Banking Law, such parties could be considered subject to the anti-money laundering obligations when carrying out "activities of conversion of virtual currencies from or into currencies with forced exchange rates" pursuant to Article 3, para. 5, letter *i)* of Legislative Decree 231/2007. See I. Bixio, 'Virtual and compliant anti-money laundering currencies: reflections on obligated subjects, new or not' (2017) Corriere tributario 2676; M. Bellino, 'I rischi legati all'ecosistema Bitcoin: i nuovi intermediari' (2018) Rivista di diritto bancario 1, pointing out that the line between one and the other was becoming increasingly blurred since 52% of *e-wallet providers* also provided *exchange* services simultaneously.

[20] D. Majorana, 'Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web' (2018) Corriere tributario 630; Di Vizio, '(n. 9), 293 ff.

Altcoins have been transferred (possibly tracing back only the IP address of the individual terminal used for sending or receiving).[21]

The Italian legislature has also shown a certain foresight and an acute sensitivity to the risk of the phenomenon, with particular attention given to the incessant and unpredictable technological growth and to the prospective centrality of a market based on solely digital and dematerialized values at the expense of the revolving doors between cryptocurrency and "real" money. The further tightening of the regulation in fact occurred with the inclusion not only of the activities made exclusively online, but also of the activities of conversion into other digital representations of value, including those in turn convertible into other virtual currencies (so-called “crypto on crypto”), alongside the more traditional services of exchange from and into currency with forced exchange rates.

In a similar approach, the Bank of Italy, in the applicative provisions on the subject of adequate verification reminiscent of Articles 17-30 of Decree No. 231/2007, recognized the crucial role of technological innovation and supported its application not only with respect to customer identification, legitimizing remote video identification and forms of biometric recognition, but above all allowing the progressive automation of certain phases of the processes designed to prevent criminal activities through the provision of sophisticated algorithms.[22]

In this regulatory framework, there has been corresponding growth both in the use of new ways of identifying and verifying data acquired remotely and in the investment of financial intermediaries in projects based on new technologies (including experimentation with forms of Artificial Intelligence such as Machine Learning and neural networks) to make the procedures related to the profiling of the risk of money laundering and illegal financing of customers, as well as the traceability, selection, classification and monitoring of anomalous operations more efficient and effective.[23]

“Anti-Money Laundering in Bitcoin has to deal with imperfect knowledge of identities but may exploit perfect knowledge of all transactions”.[24] The incisive assertion on the ambiguous nature of the cryptocurrency *par excellence*, such as to encompass perfect transparency and imperishable registration of objects with forms of concealment (of the identity of) subjects, from the most vulnerable pseudonymity to full and irreversible anonymity, justifies the separate consideration of the plausible benefits that from the use of bitcoins and, more generally, of Bitcoin/*blockchain* technology, can redound to the benefit of the entire financial system, without exception for policies to combat money laundering and the financing of terrorist activities.

In argumentation regarding the nature of fully traceable technology, that is therefore entirely transparent, impossible to falsify and difficult to steal, a recent study has theorized a re-evaluation of bitcoins as a tool not to accommodate, but rather to

[21] Capaccioli (n. 5), 253 ff.

[22] See <https://bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/ 20190730-dispo/index.html>

[23] Banca d’Italia, *Indagine Fintech nel sistema finanziario italiano*, December 2019. The *Conclusions* of the second survey on Fintech's investments in the Italian financial system state that, with a view to “increasing automation ... even the anti-money laundering legislation has favoured technological choices based on AI logic, mainly through Machine Learning applications”.

[24] Möser, Böhme and Breuker (n. 11).

counter, the numerous crimes committed with cash.[25] In asserting that the abolition of the legal currency in favor of a system based on competing digital currencies would bring enormous benefits related to the consequent superfluity of the banks, the disappearance of inflation and institutionally-driven financial crises, and the disappearance of multiple criminal cases connected with the circulation of money, the theory seems to echo the utopias and anarchic ideals of the *Cypherpunk* movement, which certainly did not lack ominous threats.[26]

The undeniable contribution that the new disruptive technology could make in terms of security and reliability to the financial system remains linked to the objective traceability of the structure, i.e. to the fully or partially public accessibility of the *database* on which all the transactions between users – the blocks of the chain – have been shared and registered in an indelible, non-retractable and unmodifiable manner. However, only the introduction of a regulatory apparatus capable of avoiding, or at least reducing, the risks connected with the lack of subjective traceability can prevent the potential benefits from being fatally compromised, cancelled out by the creation of the environment that is ideally suited for the commission of crimes that it intended to prevent.

3. *Fintech, European GDPR and personal data processing: Private profiles of traceability*

The regulatory dilemma posed by the *Fintech* phenomenon cannot be resolved by relying entirely on the solutions offered by technology, if not at the price of an unacceptable abdication to the principles of certainty and protection of the interests that each organization deems worthy of protection: on the other hand, the choice to impose traditional capillary controls and to dictate strict rules that do not take into account the structural, elusive specificity of technological innovation and its unstoppable evolution, would prove to be completely inadequate in its attempt to govern an elusive phenomenon according to traditional logic (and categories).[27] Any regulation cannot therefore ignore certain steadfast characteristics: supranational and

[25] On the functioning of technologies capable of revealing the identity of those hidden by the alphanumeric code of cryptographic keys, see P. De Filippi, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) Journal of Peer Production <http://peerproduction.net/editsuite/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/>.

[26] "Two people will be able to exchange messages, do business and negotiate contracts completely anonymously, without needing to know each other's real name or legal identity. […] The state will obviously try to stop or slow down the development of this technology, citing national security problems or the use of this technology by drug traffickers and tax evaders. Many of these concerns will be well-founded: 'cryptoanarchy' will allow free trade in state secrets and will also allow trade in illicit or even stolen goods. An anonymous computerized market will make possible a reprehensible trade in murder and extortions. Criminals and other elements extraneous to our value system will become active users of CryptoNet. But this will not stop cryptoanarchy. […] Cryptoanarchy will create a liquid market for every possible type of merchandise." See: E. Hughes, *A Cypherpunk's Manifesto*, 9 March 1993, also found online at <https://activism.net/>; see also Capaccioli (n. 5), 40 ff.; P. Franco, *Understanding Bitcoin. Cryptography, Engineering and Economics* (Padstow 2014) 160 ff.; M. Atzori, *Blockchain Technology and Decentrated Governance: Is the State Still Necessary?* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713>.

[27] "There remains the need to regulate behaviour and activities in order to avoid that everything that is technologically possible, is also and only for this reason, legally sanctioned": Giuliano (n. 1), 992 ff.

cross-border dimensions in order to support the global purpose of the regulated phenomenon, awareness and close correlation, even if not renounceable, with technological architecture and its foreseeable progress, creation of spaces in order not to hinder or impede its beneficial development and positive effects, as similarly recognized by the European institutions in relation to the realization of the so-called Digital Single Market.

To verify predictable and efficient solutions, it is helpful to examine the other regulatory sectors with which the *blockchain*/Bitcoin technology must be compared in order to evaluate its compatibility, i.e. the regulations on the protection and treatment of personal data as formulated by the GDPR, an acronym for *General Data Protection Regulation*, the EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data, which in Italy made it necessary to adapt the Legislative Decree No. 196/2003 containing the code regarding the protection of personal data, implemented by Legislative Decree No. 101/2018.[28]

From an initial point of view, the positive effects of the development of *blockchain* technology with respect to the protection of personal data cannot be underestimated, since its use can guarantee both security, in terms of integrity and inalterability, and correct management, in terms of control of accessibility and circulation, in full accordance with the approach of the Regulation. The European institutions themselves have not failed to strongly emphasize this point, in particular the Parliament which, in its *Resolution of 3 October 2018 on Distributed ledger technologies and blockchains: building trust with disintermediation* has recognized it as an instrument capable of strengthening the autonomy of citizens by giving them the opportunity to control their own data and decide which to share in the registry, as well as the ability to choose by whom and how that data can be seen.[29]

However, a comparison with the multiple new European regulations shows that there is true collision between the operation of *blockchain* technology, the circulation and movement of cryptocurrency and, more generally, the financial operations attributable to *Fintech* and the rules aimed at ensuring a high level of protection of personal data.[30]

[28] V. D'Antonio, G. M. Riccio and S. Sica (eds.), *La nuova disciplina europea della privacy* (Padova 2016); G. Finocchiaro (eds.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna 2017); L. Califano and C. Colapietro (eds.), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/279* (Napoli 2017); G. D'Acquisto and M. Naldi (eds.), *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza* (Torino 2017).

[29] European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), P8_TA(2018)0373. On point, see M. Finck, *Blockchain regulation and Governance in Europe* (Cambridge 2018) 113 ff.; Y. Zhao and B. Duncan, *The impact of cryptocurrency risks on the use of blockchain for cloud security and privacy*, 2018; M. Berberich and M. Steiner, 'Blockchain technology and the GDPR: how to reconcile Privacy and Distributed Ledgers?' (2016) European Data Protection Law Review 425; Guy Zyskind and Oz Nathan and Alex Pentland, *Decentralizing privacy: using blockchain to protect personal data,* in *IEEE CS Security and Privacy Workshops* [2015]. See also: A. M. Gambino and Ch. Bomprezzi, 'Blockchain e protezione dei dati personali' (2019) Diritto dell'informazione e dell'informatica 628.

[30] Capaccioli (n. 5), 29 ff.; Matthias Berberich and Malgorzata Steiner, *Blockchain technology and the GDPR: how to reconcile Privacy and Distributed Ledgers?, Eur. Data Protection Law Review* [2016], p. 425 et seq.; H. Chang, 'Blockchain: disrupting Data Protection?' (2017) University of Hong Kong

In particular, the evaluation of the technical-functional characteristics and the structural repercussions in terms of traceability is reversed here and it is antithetical to the reflection on criminal law made earlier. To guarantee the confidentiality of personal data as defined by Art. 4 of the Regulation ("any information concerning an identified or identifiable natural person") is, properly speaking, the element that best concretizes the criminal unknown, while the high level of *transparency and immutability* offered by that confidentiality averts the risk of contradicting in an irreversible manner the programmatic power of control over an interested party's personal data and its circulation.

On the one hand, in fact, subjective non-traceability – thus complete *anonymity* of the parties – removes the data referable to them, possibly recorded on platforms or shared through the blocks of the chain, to the very area of application of the Regulation, thus making operations through *blockchain* perfectly compatible, in the abstract, with the strict protection provided for therein (Art. 1, Reg. (EU) 679/2016).[31] On the other hand, the imperishable objective traceability of transactions – along with the distributed nature, the free accessibility, and the transparency of the system – strongly threatens the individual rights to protect their personal data, to control its circulation and to the limit the methods and purposes of its treatment (Articles 5-7, Reg. (EU) 679/2016). They also conflict with the principles granting the right that data be stored "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (Art. 5(1)(e), Reg. (EU) 679/2016); the right to correct inaccurate personal data and to supplement incomplete data (Art. 16, Reg. (EU) 679/2016); and finally, the right to the erasure without undue delay of personal data when no longer necessary with respect to the purposes for which they were collected or processed, or in case of revocation of the consent given for the processing, or of subsequent opposition, or even in the event of unlawful data processing (Art. 17, Reg. (EU) 679/2016).[32]

The perspective adopted by the GDPR supports the conceptual passage involving the protection of privacy moving from a proprietary model, based on consent, towards a procedural model, based on control and management, and favoring a pragmatic approach that aims at to establish an *ex ante* protection with respect to the inexorable, massive, systematic, and even extraterritorial circulation of personal data[33].

According to Art. 25 of the Regulation, one of the main measures for the prevention in the protection of personal data is entrusted to the rule of *data protection by design*, which accompanies that of *data protection by default*. The first rule refers to the

Faculty of Law Research Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3093166> acccessed 18 September 2020; Giuliano (n. 1), 1011 ff.; Gambino and Bomprezzi (n. 29), 619 ff.

[31] C. Del Federico and A. R. Popoli, 'Disposizioni generali', in G. Finocchiaro (eds.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna 2017) 65 ff.

[32] Users can always insert data on the chain that is incompatible with the previously entered data, which, however, would still remain visible.

[33] I. A. Caggiano, 'Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali' (2018) Osservatorio del diritto civile e commerciale 67. The supranational dimension of the discipline is ensured by a territorial scope of application that *ex* Art. 3 of the GDPR transcends the European Union, through the provision of an operation that covers the processing of personal data of subjects located in the Union, even if carried out by a data controller or processor not established within the Union (as well as processing outside the EU by a data controller or processor established in the Union).

obligation to prepare adequate technical and organizational measures right from the *design phase* of products and services which, taking into account the state of the art and implementation costs as well as the nature, scope of application, context and purposes of the processing, implement solutions capable of protecting *ex ante* both the confidentiality of data and the security of individuals. The second term refers to the provision of adequate technical and organizational measures which, *by default*, guarantee both the selective collection of only the personal data necessary for each specific purpose of the data processing, and the prevention of indiscriminate access to an indefinite number of natural persons [34]. The same rule expressly adds (and even by way of example: see Recital 28), to the range of technical and organizational measures suitable for implementing *data protection by design*, namely the "*pseudonymisation*" of data defined as follows: pursuant to Art. 4(5), the processing carried out in such a way that personal data can no longer be attributed to a specific data subject without the use of additional information, stored separately, and measures to ensure that the data cannot be attributed to an identified or identifiable natural person.

Privacy by design is a legal principle which encapsulates a paradigm that can be extended beyond the boundaries marked by the protection of personal data: as a discipline that uses technology to regulate the technology itself and that, in addition to providing a form of preventative protection which can be modulated in relation to the historical moment and the state of knowledge and applications, it transposes the empirical data without being overwhelmed by it, and appears capable of achieving regulatory convergence in order to create a desirable and necessary uniform framework at the supranational level[35].

The intention is not to uncritically extend to sectors governed by other principles – for the protection of other interests – a precept for the prevention of well-identified and circumscribed risks, or to recognize that it is complete and resolutely effective response to any situation in which the technological innovation applied to finance threatens interests worthy of protection, nor the choice for an inseparable and self-sufficient *Fintech/Regtech* combination, but rather to understand the value of a regulatory model equipped with many of the essential requirements for efficient protection and a promising degree of elasticity.

[34] R. D'Orazio, 'Privacy by design e by default', in V. D'Antonio, G. M. Riccio and S. Sica (eds.), *La nuova disciplina europea della privacy* (Padova 2016) 81 ff.

[35] M. C. Gaeta, 'La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi' (2018) *Diritto dell'informazione e dell'informatica* 147, 177, speaks of *techno-regulation*. "The speed of technological evolution and globalization pose new challenges for the protection of personal data. The scope of sharing and collecting personal data has increased significantly. Current technology allows both private companies and public authorities to use personal data, as never before, in carrying out their activities. Increasingly, individuals make personal information about themselves available to the public worldwide. Technology has transformed the economy and social relations and should further facilitate the free movement of personal data within the Union and its transfer to third countries and international organizations, while ensuring a high level of protection of personal data. This evolution requires a more solid and coherent data protection framework in the Union, supported by effective implementation measures, given the importance of creating the climate of trust that will allow the development of the digital economy throughout the internal market. Individuals should have control over their personal data and that legal and operational certainty should be strengthened both for natural persons and for economic operators and public authorities." Thus, effectively and with a clear awareness of the technological factor, see Recitals 6-7 of Regulation (EU) 679/2016.

Among the options to "integrate safeguards in data processing" in order to achieve the purposes underlying the adoption of the Regulation, the rule identifies, on the basis of Recital 78 and also by way of example, the processes aimed at the minimization and pseudonymisation of personal data.[36]

Pseudonymity differs from anonymity in that the masking of identity is not definitive but reversible, allowing the identification of the real center of interests (those to whom the personal data refer or the persons, natural or legal, who have concluded transactions by disposing of or receiving cryptocurrency), thanks to the use of further elements or "additional information" with which to overcome the cryptography and associate the keys to one - and only one, unequivocal - identity. The technical methods of *pseudonymisation* do not interrupt the concatenation of the steps necessary for the connection between data and person, but rather make their identification more or less complex and easily traceable. In other words, "the one-to-one association between data and person is not modified ... and the pseudonymous data, once used in combination with all the tools necessary to perform the replacement of attributes in reverse, is unequivocally referable to the person".[37]

Clearly, not every dilemma is settled, nor every critical profile eradicated, nor every threat that could arise from applying technology to finance eliminated. The operational difficulties and mechanisms, even those technological in nature, preventing a reliable re-identification have already been highlighted: and there is no doubt that much of the effectiveness depends on the availability and ease of use, even in terms of costs and time, of the measures with which the identity of the interested parties or really concerned parties can be traced. Technical measures for prevention – of the commission of crimes or the illegitimate treatment of data - destined to evolve together with the same technology used to support the phenomena to be prevented, should be easily accessible by the National Financial Intelligence Units in order to assess its reasonableness (as underlined by the GDPR) and for the purpose of preventing the use of the financial system for the purpose of money laundering or terrorist financing, as required by the Fifth EU Directive.[38]

The tensions between confidentiality and transparency, protection of personal data and general security, the aim of protecting personal privacy on the one hand and the prevention of crimes and security of the financial system as a whole on the other remain in the background, seemingly unsolvable: in a prospective view, even analogous personal identity is destined to fade towards digital identity. In *pseudonymity* – a masking capable of making the persistent unequivocal correspondence between data and person not immediately intelligible, reversible because it is tempered by adequate methods of identification *a posteriori* where necessary – it seems, however, that security objectives and principles of privacy can converge, without the safeguarding of the one annihilating the defense of the other or a set of interests systematically prevailing over the other.

[36] On the technical modalities of anonymisation and pseudonymisation of data, see D'Acquisto and Naldi (n. 28), 41 ff. and 117 ff.

[37] Ibid., 38.

[38] Gambino and Bomprezzi, (n. 29), 630, about applications suitable for preventing the multiplication of digital identities (accounts) facing a single analogue identity (*Sovrin, Evernym*) and authentication systems designed to create an ID, with one's personal data, to be included in the blockchain in a reliable and inaccessible way (*ShoCard*).

In all likelihood, the best performance by the technical measure (and of the underlying regulatory paradigm) could be guaranteed by the retention of the additional *off-chain* information, making it all the more secure when entrusted to subjects under the supervision and control of, and subject to, *compliance* systems, as in the case of *exchangers* and *wallet providers*. In this perspective it is equally undeniable that, unlike those *permissionless*, the *permissioned blockchains* – in which an entity or group of blocks has the prerogative to allow access to the system by admitting new nodes to contribute – can achieve a significant increase in the level of identification (or at least identifiability) of users[39].

To recognize only the lawfulness of distributed ledger systems, characterized by at least a partial hierarchical centralization (*permissioned, consortium* or *private*), or to link security and confidentiality to the *off-chain*, if not even to the tangible materiality of *off-line* devices, at this stage would mean however denying, and not regulating, the phenomena.

Despite whatever opposition or carelessness may exist, technological innovation does not stop and does not retreat, and it only reveals new scenarios, some encouraging and others challenging: scenarios that are undoubtedly difficult and hostile if the expectation is to continue to represent the world with existing categories.[40]

[39] Gambino and Bomprezzi, (n. 29), 627 ff. and 632 ff.

[40] "The ultimate revelation of the fragility of all things. Old and thorny questions had resolved into darkness and nothing. The last example of a thing carries with it the category. It turns off the light and disappears" (Cormac Mc Carthy, *La strada* (M. Testa tr., Torino 2007) 22.

BLOCKCHAIN AND THE FOOD SUPPLY CHAIN: THE FUTURE OF FOOD TRACEABILITY

PAMELA LATTANZI – SERENA MARIANI*

SUMMARY: 1. Introduction. – 2. "Blockchainizing" Food Supply Chains: Potential Applications. – 2.1. Traceability in the EU Food Legislation. – 2.1.1. Blockchain-Based Traceability in Practice. – 3. Future Challenges.

1. *Introduction*

The ability to trace foodstuffs backwards and forwards along all the stages of the supply chain is of crucial importance for assuring food safety because it empowers the competent national authorities and businesses to facilitate outbreak responses and food fraud deterrence. Accordingly, in setting out the general principles and requirements for the food safety regulation in the European Union, Regulation (EC) No 178/2002 (also known as the General Food Law, GFL) requires that food and food ingredients be traceable "from farm to fork", and therefore it imposes on food business operators (FBOs) a general obligation to ensure food traceability.

Current traceability systems face several challenges due to multiple factors such as the globalization and complication of agri-food supply chains, which are increasingly composed of many players of all sizes and abilities; the information asymmetry in the market, as well as the great reliance upon paper-based record keeping, susceptible to mistakes and vulnerable to fraud, or upon internal computer systems, which make data unusable for other companies and cause difficulties for stakeholder integration.[1]

Many technological innovations are in place for tackling such challenges, among them blockchain technology which is gaining substantial attention because it is not only "a way to efficiently pass down along the supply chain the traceability information" (like QR-codes and RFDI), but it also "helps to endorse the credibility of the information", in doing so it "provides the agri-food market with a trustworthy framework in which to store every passage of the production and distribution chain".[2]

* Despite the chapter's unitary conception, Pamela Lattanzi drafted Section 1 and Subsection 2.1, while Serena Mariani drafted Section 2, Sub-subsection 2.1.1 and Section 3.

[1] S. Pearson and others, 'Are Distributed Ledger Technologies the Panacea for Food Traceability?' (2019) 20 Global Food Security 145; Ching-Fu Lin, 'Blockchainizing Food Law: Promises and Perils of Incorporating Distributed Ledger Technologies to Food Safety, Traceability, and Sustainability Governance' (2020) 74 Food and Drug Law Journal 586; G. Mirabella and V. Solina, 'Blockchain and Agricultural Supply Chains Traceability: Research Trends and Future Challenges' (2020) 42 Procedia Manufacturing 414.

[2] R. Berti and M. Semprebon, 'Food Traceability in China' (2018) 13 European Food and Feed Law Review 529.

Blockchain is a subset of distributed ledger technologies (DLTs)[3] "employing cryptographic techniques to record and synchronise data in chains of blocks".[4]

In short, it "is a distributed ledger based on a peer-to-peer (P2P) network, in which participants, called nodes, agree on a unique version of the distributed data storage through a shared consensus mechanism. All information stored inside the ledger is digitally signed employing cryptographic primitives and data-authenticity is guaranteed by the use of asymmetric key-pairs".[5]

There are many different blockchain technologies with distinct technical and functional configurations as well as internal governance structures.[6] Moreover, blockchain technology may be combined with other innovative technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI), and it can also be used as a programmable platform that enables new applications such as smart contracts (i.e. self-executing software code).[7]

The main blockchain features – decentralization, tamper-resistance, transparency, and security[8] – make it one of the best promising solution to food traceability issues and, more in general, to food supply chain management issues. However, it is still in its early stage of development and several open challenges need to be addressed before it can be widely used.

This paper, therefore, aims to investigate the potential of blockchain technologies in revolutionizing food supply chains. It will analyse the benefits and challenges of blockchain adoption in food supply chains, especially for traceability purposes.

2. *"Blockchainizing"[9] Food Supply Chains: Potential Applications*

Food chains are complex and vulnerable systems. They are composed of multiple stages and made up of different operators and processes, covering food production, transport, distribution, marketing, and consumption,[10] which have become even more

[3] 'DLTs are particular types of databases in which data is recorded, shared and synchronised across a distributed network of computers or participants', S. Nascimento and A. Polvora (eds), *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies* (Publications Office of the European Union 2019) 13.

[4] Ibid.

[5] J. Grecuccio and others, 'Combining Blockchain and IoT: Food-Chain Traceability and Beyond' (2020) 15 Energies 2.

[6] "They can be distinguished depending on who can read, execute and validate transactions. When anyone can read and access a blockchain it is categorised as "public" or "open" which means that anyone can access a whole blockchain and read its contents. When only authorised entities have access, a blockchain is considered closed or private. Blockchains can be further categorised as 'permissionless' or 'permissioned' depending on who can send transactions and who can validate them. If anyone can send and validate transactions, the blockchain is called permissionless. If entities need to be authorised to execute or validate transactions, or both, the blockchain is called permissioned'. Moreover, hybrid blockchains may combine different aspects. Nascimento (n 3) 14.

[7] Spark Legal Network and others, *Study on Blockchains: Legal, Governance and Interoperability Aspects. A Study Prepared for the European Commission DG Communications Networks, Content & Technology* (Publications Office of the European Union 2020).

[8] Nascimento (n 3) 16.

[9] Lin (n 1).

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Farm to Fork Strategy. For a Fair, Healthy and Environmentally-friendly Food System, COM(2020) 381 final, 20 May 2020, para. 2.

complex with globalisation and outsourcing.[11] The vulnerability of the value-added chain of agricultural and food products requires great attention and remarkable efficiency in order to ensure high safety and quality standards at the lowest possible cost.[12]

Currently, the management of food supply chains is associated with numerous challenges such as information disclosure, risk assessment and management, product tracing, food fraud, consumers' trust and stakeholders' reputation.

In this context, blockchain can help simplify these challenging tasks. Blockchain is designed to be decentralized and irreversibly store data, thus it represents an interesting solution to classic and often outdated databases based on centralized systems, which lack trustworthiness due to the higher risk of data tampering.[13]

More specifically, blockchain-based food chains have the potential to improve transparency, efficiency, and safety.

Transparency is highly valued by public and political agendas and demanded by civil society. Information disclosure in the food chain is particularly crucial for companies in order to maintain consumers' trust.[14]

The advantages of applying blockchain for transparency purposes rest on the irreversibility of information along the chain: once data have been stored and verified, they are immutable. In fact, companies cannot modify or select data that are beneficial to their own reputation without altering the entire blockchain history.[15] These data are equally and instantly available to all the operators involved, creating a direct link among them along the supply chain.

The information captured in a blockchain can be used to establish many food attributes, such as provenance, ingredients, allergens, safety, quality, and consumers can depend on smart labels to access information, increasing the trustworthiness of the brands.[16]

Transparency is also important in the field of the environment and sustainability: a blockchain-based supply chain enables a circular economy since it gives consumers confidence about the origin of the food or whether the packaging is recycled or first-use.[17]

The rise in efficiency due to the adoption of blockchain is achieved through the use of smart contracts and the combination with the latest IoT technologies.

[11] J. Duan and others, 'A Content-Analysis Based Literature Review in Blockchain Adoption within Food Supply Chain' (2020) 17 International Journal of Environmental Research and Public Health 1784.

[12] H. Folkerts and H. Koehorst, 'Challenges in International Food Supply Chains: Vertical Co-ordination in the European Agribusiness and Food Industries' (1998) 100 British Food Journal 385.

[13] G. Baralla, A. Pinna and G. Corrias, 'Ensure Traceability in European Food Supply Chain by Using a Blockchain System', in *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain* (IEEE 2019).

[14] A. Mol, 'Transparency and Value Chain Sustainability' (2015) 107 Journal of Cleaner Production 154.

[15] J. Galvez, J. Mejuto and J. Simal-Gandara, 'Future Challenges on the Use of Blockchain for Food Traceability Analysis' (2018) 107 Trends in Analytical Chemistry 222.

[16] G. Spoto, 'Gli Utilizzi della Blockchain e dell'Internet of Things nel Settore degli Alimenti' (2019) 13 Rivista di diritto alimentare 25.

[17] R. Casado-Vara and others, 'How Blockchain Improves the Supply Chain: Case Study Alimentary Supply Chain' (2018) 134 Procedia Computer Science 393.

The use of smart contracts can increase efficiency because of their self-executing nature. In particular, smart contracts remove intermediaries, rapidly evaluating, certifying, and allowing trusted transactions among operators without the need for a central authority.[18]

In addition, the combination with IoT devices creates an efficient and high-speed network along the supply chain: sensors reduce manual errors by automatically capturing and storing real-time information about a product (e.g. quantity, temperature, humidity). Reliable and real-time data flows are very important especially for frozen and fresh food since their quality is easily affected by outer environments.[19]

With respect to safety, during the past decades many food scandals and foodborne disease outbreaks have been reported and this is the reason why consumers are extremely concerned about food safety.[20]

Public health and food safety issues can be more easily addressed by blockchain technology:[21] the efficient collection of critical data along the chain allows quality checks during all the different stages of food production, transport, distribution, and marketing. By way of illustration, blockchain offers a solution to the problem of checking the maintenance of adequate cold chain conditions during production, transport and storage of frozen and perishable foods, conditions that are critical to food safety.

Moreover, the use of blockchain protocols facilitates and speeds up the complicated food recall process through traceability mechanisms.

2.1. *Traceability in the EU Food Legislation*

According to the General Food Law, the fundamental goal of food traceability is the removal of unsafe food from the market. In addition, traceability could help to ensure fair trading amongst operators as well as the reliability of information supplied to consumers in terms of substantiating claims made by manufacturers. To these ends, mandatory requirements for traceability are set out in Art. 18 GFL, which applies to all food and ingredients placed on the EU market.[22]

In line with the principles of food traceability laid out in international standards provided for the Codex Alimentarius, Art. 18 GFL embraces the "one step back-one step forward" approach. Therefore, it requires that FBOs are able to identify any person from whom they have been supplied with a food/raw material and to whom their products have been supplied (excluding final consumers). "The burden of reconstructing the whole food chain when an incident occurs is on the authorities and to that end traceability information has to be made available to those authorities on demand".[23] Consumers are not necessarily provided with traceability information,

[18] Baralla (n 13).

[19] Duan (n 11).

[20] K. Demestichas and others, 'Blockchain in Agriculture Traceability Systems: A Review' (2020) 10 Applied Sciences 4113.

[21] Q. Lin and others, 'Food Safety Traceability System Based on Blockchain and EPCIS' (2019) 7 IEEE Access 20698.

[22] Art. 18 also applies to feed traceability. Additional requirements are laid down in other normative acts for specific food categories.

[23] B. Van Der Meulen (ed.), *EU Food Law Handbook* (Wageningen Academic Publisher 2014) 360.

since "traceability is conceived as a step-by-step process: information is not required to follow the entire production process and distribution chain through to the market, but is rather confined to the specific stage of the production concerned".[24]

It is important to note, that "article 18 is worded in terms of its goal and intended result, rather than in terms of prescribing how that result is to be achieved".[25] The design of the traceability system is up to FBOs and it is also left to their discretion to put in place internal traceability (aimed at establishing a link between incoming and outgoing products) and the level of detail of the adopted traceability system.[26]

Recently, the Commission has concluded the Fitness Check on the General Food Law Regulation, which also covers the implementation of mandatory traceability requirements.[27]

The results of the analysis point out that the EU-wide traceability has significantly contributed to assuring food safety. The superiority of the EU traceability system vis-à-vis other non-EU countries is also underlined.

Nevertheless, the assessment reveals that there are some aspects that could be improved, since "it still occurs that the traceability chain is interrupted because of errors or incomplete documentation at a particular stage".[28] Moreover, it is reported that the EU-wide traceability does not always result in targeted withdrawals when the risk involved with suspected products is considerable.

Even if the EU-wide traceability is not perceived as burdensome by the majority of FBOs, who believe that the benefits of mandatory traceability outweigh the corresponding costs, a significant part of consulted businesses (in particular SMEs) ranked the cost of traceability compliance (together with labelling, authorisations, registration, and certification) as one of the most costly of all EU food law requirements. This high cost could depend on the fact that the majority of SME respondents have in place more extensive traceability systems than what is required by the GFL Regulation, with a direct impact on the increased administrative burden.[29]

Many studies underline that blockchain technology may help in overcoming such limitations and improving the benefits of traceability.

2.1.1. *Blockchain-Based Traceability in Practice*

Blockchain can efficiently satisfy all traceability requirements in all stages of the food supply chain. By using blockchain technology, the system can establish a collaborative network of trustworthy information from farmer to consumer. The movements of products are recorded by each operator along the chain and the network contains all the data flow about a final product and its origin. Moreover, the adoption of blockchain protocols could quickly trace single ingredients along the

[24] L. Salvi, 'Traceability and Hygiene Package' in L. Costato and F. Albisinni (eds) *European and Global Food Law* (Wolters Kluwer 2016) 285.

[25] Guidance on the Implementation of Articles 11, 12, 14, 17, 18, 19 and 20 of Regulation (EC) N° 178/2002 on General Food Law, Conclusions of the Standing Committee on the Food Chain and Animal Health, 26 January 2010, 17.

[26] Ibid.

[27] European Commission, Commission Staff Working Document the Refit Evaluation of the General Food Law (Regulation (EC) No 178/2002), SWD (2018) 38 final, 15 January 2018.

[28] Ibid.

[29] Ibid.

chain and verify the compliance of foods with their labels (i.e. food authentication), saving time and unnecessary costs.

One of the most well-known applications of blockchain in the food chain for traceability purposes is IBM Food Trust. In 2016 a pilot study was conducted in collaboration with Walmart to trace mangoes and Chinese pork from the final product to its origin. The study has shown that IBM Food Trust can significantly reduce the traceability time: the identification of the provenance of mangoes was reduced from approximately 7 days to 2.2 seconds. Currently, IBM is collaborating with many big food companies, such as Nestlé and Driscoll's, to identify new fields that can benefit from blockchain application.

In the past years, other pilot studies have been carried out by AgriDigital in the Australian grain industry, Provenance in the fish industry and AgriOpenData for biological food.

Following these leading studies, nowadays many startups, companies, and universities are creating solutions in the field of food traceability by using blockchain.

For example, Moyee Coffee is developing a system from Ethiopia to Europe to track coffee in a transparent manner. Seville University is testing a project named Olivacoin in order to minimize abuses and frauds in the olive oil sector. In China, ZhongAn is using blockchain to monitor the life of chickens on organic farms to address consumers' concerns. In Europe, Carrefour launched a blockchain information network for fresh products, such as oranges and lemons, to ensure greater traceability. In the area of frozen food, Bofrost has started to use blockchain to trace cod fillets and artichoke along the cold chain.

3. *Future Challenges*

In the European Union, food should be traced and tracked in all production, processing, and sales stages: an efficient traceability system provides an exact recording of product movements. However, the existing systems make it impossible to easily find out the entire product's movements along the chain.[30]

In this framework, executing food traceability by using blockchain has numerous benefits in terms of time saved, reduced costs and risks as well as increased trust[31]. The immutable and real-time data flow improves the visibility of the movement of products across the entire supply chain, thus speeding up the tracing process in an efficient, reliable, and transparent manner, allowing food authentication and targeted food recall for the benefits of operators and consumers. The adoption of blockchain could increase the trust of consumers and civil society in a brand and could be used as a tool for building strategic partnerships among stakeholders.

However, blockchain is not a panacea for all problems. It should be considered that there are a number of technical and regulatory challenges.

First of all, the food supply chain is made up of a large number of stakeholders from different and distant geographical areas, whose technological knowledge may be

[30] R. Scharff, 'State Estimates for the Annual Cost of Foodborne Illness' (2015) 78 Journal of Food Protection 1064.

[31] Galvez (n 15).

significantly diverse and who may be reluctant to adopt costly and not well-understood technologies.[32]

Moreover, blockchain has low scalability and cannot store an indefinite amount of data: the recording of a great number of data can slow down the network and the speed of validation. Furthermore, blockchain technology may not offer an added value to the existing food chains, especially to short food supply chains.[33]

In this challenging context, the legal framework has to be updated in order to safeguard consumers' rights and protect companies' intellectual property (IP), especially trade secrets. In fact, the adoption of blockchain technology cannot eliminate the risk of raw data manipulation by operators before their upload into the system, to the detriment of consumers: the authenticity of the initial data is not guaranteed by the use of blockchain. Also, the uploading of confidential information in the blockchain could lead to misappropriation of trade secrets by other operators, thus undermining the company's assets. Therefore, the law has to provide effective tools to protect IP in the blockchain era.

Furthermore, compliance between agreements and smart contracts needs to be ensured: the consequences of errors in smart contract design have to be addressed in order to avoid damage to business relations among stakeholders.[34]

Considering the remarkable investments required to develop a blockchain-based supply chain, another great challenge is to identify who owns each blockchain infrastructure, who owns the collected data, and to establish privacy mechanisms[35]. The law also needs to determine data standardisation in the food domain and to set a legal minimum for how long blockchain-based traceability records must be kept and by whom so that data are correctly archived.[36] Lastly, the legal framework needs to set common standards that can facilitate data collection in blockchain-based food supply chains across international borders and jurisdictions.[37]

In conclusion, the food sector is in a key position for exploring the potential of blockchain but it is necessary to design a strong digitalisation strategy for agrifood businesses, to develop common standards for the blockchain implementation, and to design a clear regulation for blockchain-based food chains: the creation of a better regulatory environment is fundamental for "blockchainizing" food law.[38]

[32] Demestichas (n 20).

[33] Lan Ge and others, *Blockchain for Agriculture and Food. Findings from the Pilot Study* (Wageningen Economic Research 2017).

[34] Ibid.

[35] Pearson (n 1) 148.

[36] Ibid.

[37] M. Tripoli and Joseph Schmidhuber, *Emerging Opportunities for the Application of Blockchain in the Agri-food Industry* (FAO and ICTSD 2018) 21.

[38] Lin (n 1).

LIST OF AUTHORS

ROBERTO ACQUAROLI – *Department of Law, Università di Macerata*

TAMIR AGMON – *Professor Emeritus, University of Tel Aviv*; *Seamless Logic Software Ltd*

DANIELE AMOROSO – *Department of Law, Università di Cagliari*

ALESSIA ARTECONI – *Department of Industrial Engineering and Mathematical Sciences, Università Politecnica delle Marche*

MARCO BALDI – *Department of Information Engineering, Università Politecnica delle Marche*

ALESSIO BARTOLACELLI – *Department of Law, Università di Macerata*

DALILA CALABRESE – *Althena Medical*

ANDREA CALIGIURI – *Department of Law, Università di Macerata*

LEVY COHEN – *Seamless Logic Software Ltd.*

PAOLA CRICCO – *Banca d'Italia*

ENRICO DAMIANI – *Department of Law, Università di Macerata*

MARIA CONCETTA DE VIVO – *former Professor, Università di Camerino*

MICHELE FAIOLI – *Faculty of Economics, Università Cattolica del Sacro Cuore*

CHIARA FELIZIANI – *Department of Law, Università di Macerata*

EMANUELE FRONTONI – *Department of Information Engineering, Università Politecnica delle Marche*

FRANCESCO GAMBINO – *Department of Law, Università di Macerata*

PAMELA LATTANZI – *Department of Law, Università di Macerata*

ALDO LAUDONIO – *Department of Law, Economics and Sociology, Università Magna Graecia di Catanzaro*

MARCO MACCHIA – *Faculty of Economics, Università di Roma "Tor Vergata"*

ARIANNA MACERATINI – *Department of Law, Università di Macerata*

SILVIO MAGNOSI – *Department of Science and Technology, Università di Napoli Parthenope*

SERENA MARIANI – *Department of Law, Università di Macerata*

GIACOMO MENEGUS – *Department of Law, Università di Macerata*

Florian Möslein – *Institute for Commercial and Business Law and Institute for the Law of Digitization, Philipps-Universität Marburg*

Matteo Paroli – *Autorità di Sistema Portuale dell'Adriatico Centrale*

Elisabetta Pederzini – *Department of Law, Università di Trento*

Stefano Pollastrelli – *Department of Law, Università di Macerata*

Giulia Rafaiani – *Department of Information Engineering, Università Politecnica della Marche*

Cristina Renghini – *Department of Law, Università di Macerata*

Giuseppe Rivetti – *Department of Law, Università di Macerata*

Luca Romeo – *Department of Law, Università di Macerata*

Konstantinos Sergakis – *School of Law, University of Glasgow*

Francesca Spigarelli – *Department of Law, Università di Macerata*

Guglielmo Tamburrini – *Department of Electrical and Information Technology Engineering, Università di Napoli "Federico II"*

Carmen Telesca – *Department of Law, Università di Macerata*

Alfredo Terrasi – *Department of Law, Università di Palermo*

Yan Yuting – *Institute of International Law, Chinese Academy of Social Sciences*

Stefano Villamena – *Department of Law, Università di Macerata*