

Technological Transformations, Law and New Digital Culture. Block chain, Distributed Systems and Smart Contracts. Internet Service Provider Contracts in the Age of Artificial Intelligence

Gino Fontana

Pegaso Digital University, Italy
sl.gf@libero.it

Abstract

Technology and the Internet have revolutionised the way human beings do, think and act, making relationships with others, life, everyday life and even work more pleasant and simple. Man now lives with technology, he can no longer do without it and follows its constant evolution and improvement over time. This work highlights how society has accepted and adapted to this change. Today, men and women of all ages use the internet in their free time, for work, to book holidays, shop, and keep in touch with distant friends and relatives. Therefore, there are countless changes due to the introduction of new information and communication technologies. Certainly, positive changes, even if we often risk stumbling into the trap of the internet and violating the rights of others. Work has also improved with new technological and digital tools. In fact, new systems have been introduced in companies, such as Blockchain, which have improved organisational means, allowing an increase in benefits and significant improvements from every point of view, from production to external relations. We can say that today, there is no longer a distinction between man and technology since it is now part of us, of our lives and contributes to our evolution from every point of view.

Keywords: internet, media, ISPs, contracts, liability, legislative decree 70 of 2003, EU directive 31 of 2000, blockchain, artificial intelligence, smart contracts, distributed systems, technological anarchy, frequency and regulatory production, ISPs

Preamble

The revolutions, linked to technological progress that generally accompany the history of peoples are never sudden and instantaneous phenomena, but, the fruit of constant modifying actions and acceptance of change, gradual, manifesting themselves in stages, crossing a medium to long term time span that, reaching

their apex, incorporate social changes, the fruit of matured technological innovations. Law as a social science is fully invested in phenomena linked to technological implementation and progress. Indeed, technology is the means by which society changes and evolves, bringing with it the natural consequences that have always been linked to epochal transitions. The Internet has revolutionised the way human beings do, think and act, perhaps making relations with others, life, everyday life and even the way of working or interpreting work more pleasant and easier; on the other hand, it has forced the system to mutate social paradigms and the rules that govern the apparatuses. The man now lives with, and dare we say, is forced to live with, technology and can no longer do without it; he, therefore, experiences its constant evolution over time. The technological anarchy that accompanies digital evolution seems to dominate in some respects the regulatory gaps at all levels, producing a system that only apparently seems to democratise society but which, in substance, amplifies the inequality and disparity of tools and knowledge and the very protection of individuals. This work aims to highlight how society has accepted change and is 'constantly adapting' to it, also in terms of regulatory evolution. It was intended to focus the work on the relationship that exists between the new technological advances and the classic instruments of law, as well as the existing sector regulations, analysing as far as possible the evolutionary frequency of the rule with respect to the current panorama. Today, men and women of all ages use the Internet to cultivate social relationships, work, make reservations, shop of all kinds, and obtain information to inform their decisions. Thus, countless social changes have occurred due to the introduction of new information and communication technologies. The mutation of paradigms, in some respects, certainly positive, risks tripping up operators in the sector, including those of the law and users of services, in the trap of the 'absolute and at all costs' liquidity of the law 'and of the Internet' by proposing a single key of interpretation and interpretation, as the only one possible, based on general principles alone, entrusting the stipulation of protocols, codes of conduct and self-regulation to the discretion of private individuals, effectively violating the fundamental rights of citizens, relying on spurious *normative* and regulatory *grafts* from other legal cultures, which have

little to do with the regulatory system into which they are catapulted. New, high-performance technological and digital tools are leading companies and consumers to new landfalls and the use of systems, such as blockchain, smart contracts, and AI systems, which, while improving organisational means, also represent an unregulated ocean or, better still, an opaque and gloomy ecosystem in which the balance must be found. On the other hand, Internet service providers as service providers, sometimes belonging to different jurisdictions, represent the true holders of the technological infrastructures capable of influencing the reality in which they operate from economy to information. We can say that today, there is no clear-cut distinction between man and technology since the existence of one is conditioned and mediated by that of the other, just as there is no longer a dichotomous distinction between public and private law, anchored by now, to classical logic. A society devoid of rules or with an inadequate and obsolete regulatory system becomes a place of arbitrariness and only apparent freedom, where the technocracy brought by the new technologies, if on the one hand, it becomes a field of economic progress, on the other, the concentration of technological instruments, in the hands of a few, becomes a true technological dictatorship.

1. SUMMARY:

1. Introduction and preliminary remarks. -
2. Blockchain artificial intelligence and smart contracts. -
3. Internet serviceprovider contracts. -
4. Research demand. -
5. Regulatory response frequency analysis with respect to technology implementation in Italy. -
6. The European regulation on ISPs. - 7
7. The regulation in Italy on ISPs. -
8. Conclusions.

1. INTRODUCTION AND PRELIMINARY REMARKS

The birth of the Internet has marked our existence. Rapid has been its evolution and its taking root within society. It was 1969 when the Arpanet project connected four computers, those of three Californian universities (Los Angeles, San Francisco and Santa Barbara) and the University of Utah¹. The 1970s and 1980s saw the transition from the Arpanet to the Internet, ushering in an era that would forever change our existence and the way we communicate and stay connected to the rest of the World². Italy was the fourth country in Europe to be connected to the Internet in 1986, after Norway, the United Kingdom and Germany, thanks to funding from the US Department of Defence. From the University of Pisa's Centro Nazionale Universitario di Calcolo Elettronico, hometo one of the most advanced research groups in Europe, a connection was established with CERN in Geneva on 6 August 1991, giving birth to the World Wide Web. The technology was officially made public two years later, thus opening up access to the Internet to millions of people³. Today, we find it difficult, if not impossible, to live without the Internet. Staying disconnected would mean being estranged, out of the world, just like a fish out of water. Through the net, we communicate, work, book trips, feed our hobbies and indulge in moments of relaxation⁴. The fundamental role that the Internet plays in our lives is demonstrated by the revolution in the field of work when the pandemic forced us into the biggest experiment in smart working in order tokeep society functioning. Schools were closed, but students were able to continue learning through distance learning, albeit amidst freeze-framed images and mishaps. Even though the pandemic forced us indoors, video calls with Zoom, Skype and Google Meet gave us the excitement of sharing aperitifs, dinners, and even watching a film⁵. From online concerts and museums to

¹CASTELLS M., *Internet Galaxy*, la Feltrinelli, 2006 ²MARRELLA F., *International Trade Law*, CEDAM, 2023³CASTELLS M., *Op. cit.*

⁴CANTONI L., TARDINI S., *Internet*, Routledge, 2006.

⁵TURKLE S., *Life on the Screen. New identities and social relations in the age of the Internet*, APOGEO, 1997.

Instagram feeds and the Internet have proved to be the best allies we could hope for in times of pandemic⁶. Thus, there are countless changes due to the introduction of new information and communication technologies⁷. Not only the way of communicating, approaching the world, studying and working has changed, but also economic and trade relations as well as those between public administrations⁸. All states in the world, from the most developed to the least developed, are experimenting with new political strategies in order not to be unprepared for the change⁹. With the spread of computers and, consequently, the development of communication systems capable of presenting information in its various forms (voice, sound, text, image), there is a tendency to emphasise the importance of communication, thus giving rise to the concept of the 'information society'¹⁰. Given the many unknowns and fragilities of a constantly evolving community, the emerging society can have positive as well as negative implications¹¹. Certainly, the information and/or algorithm society has improved the quality of life and services related to health, leisure, entertainment, shopping and schooling¹². At the same time, however, it has significantly increased the public power of economic planning, in stark contrast to the liberalism that has so far produced the development of new technologies¹³. Recent ISTAT studies have shown that, in the EU, women use the net more than men to interact on social networks, make phone calls or buy clothes. In contrast, men read more news, use internet banking and buy electronics and films online. On the other hand, when it comes to buying tickets for events, booking travel and accommodation,

⁶BUFFARDI A., *Futuri possibili: Formazione, innovazione, culture digitali*, Egea, 2022.

⁷FRIGERIO C. - RAJOLA F. - CARIGNANI A., *ICT and the Information Society*, McGraw-Hill Education, 2010.

⁸QUATTROCIOCCHI W. - VICINI A., *Misinformation: A Guide to the Information and Credulity Society*, Franco Angeli Editore, 2016.

⁹PARADISO M., *Geography and Spatial Planning in the Information Society*, Franco Angeli Editore, 2003.

¹⁰PIETRANGELO M., *La società dell'informazione tra realtà e norma*, Giuffè Editore, 2007.

¹¹LUCARELLI S., *La società dell'informazione: problemi e prospettive*, << Informatica e Documentazione >>, 1998.

¹²CALIGIURI M., *Public Communication, Education and Democracy. Percorsi per l'educazione del cittadino nella società dell'informazione*, Rubbettino, 2005.

¹³MOROZOV E., *The Naivety of the Net - The Dark Side of Internet Freedom*, Giappichelli, 2011.

there are no differences between men and women as well as when it comes to sending and receiving e-mails and searching for jobs.

Today, almost everywhere, two different categories of people are emerging: those who use and those who do not use the Internet. The former are those who have the possibility of accessing this resource because they work in large companies that make use of the Net or because they attend schools and universities where the connection represents an important learning tool or those who live in realities where access to the Internet is cheap or even free¹⁴.

Non-users, on the other hand, are all those who cannot afford a connection either for economic reasons or because they live in environments where they do not yet have the necessary computer skills to access the Internet¹⁵. Therefore, in order to avoid a disparity between users and non-users, the connection costs should be reduced¹⁶. This is because new poverty and illiteracy could arise from those who cannot access electronic information due to lack of means¹⁷. But this is only one of the many problems produced by the information society. In fact, in such an avant-garde reality, the excessive and perverse use of technology is undermining a fundamental right such as the right to property¹⁸. Thanks to the Internet, in fact, everyone has free access to a vast amount of information practically free of charge, as well as the possibility of filming, reproducing or transforming everything that passes through the network¹⁹. This opportunity is offered by technology and is strictly in contradiction with the provisions of Article 27 of the Universal Declaration of Human Rights. The first paragraph of this article states

¹⁴Statistics Report ISTAT, 17/03/2023.

¹⁵CARR N., Does the Internet make us stupid?: How the Net is changing our brains, Raffaello Cortina Editore, 2013.

¹⁶CAMUSSONE P.F. - OCCHINI G., Il costo dell'ignoranza nella società dell'informazione, Mondo digitale, 2003.

¹⁷SARTORI L., Il divario digitale: Internet e le nuove disuguaglianze sociali, Il Mulino, 2006.

¹⁸ROSSELLI R., Le prospettive dello sviluppo socio-economico di Internet, in << Informatica e Documentazione >>, 1998.

¹⁹ROSSI G., La proprietà caduta nella rete, Corriere della Sera, 02/12/2004.

that everyone has the right to participate in the cultural life of the community, to enjoy the arts, and to take part in the progress of science and the positive events that result from it, while the second paragraph states that every human being has the right to be protected in his or her material and moral interests resulting from literary, scientific or artistic production²⁰. With the access to the Internet, protecting intellectual property with respect to property rights and freedom rights has become very difficult, if not almost impossible²¹. The origins of intellectual property are not recent. The sculptor Benedetto Antelami was the first to sign one of his works back in 1178, while the Republic of Venice granted the first copyright to the printer of the Histories of Pliny the Elder²². The idea stems from the hypothesis that if there is a value, then there must necessarily also be a right, and it is precisely for this reason that the concept of a patent to protect inventions was introduced into our legal system²³. In this way, protection applies not only to the creativity and publication of works of art on paper but also extends to the possibility of turning a play into a book, broadcasting it on television, or reproducing the works of great musicians and artists on radio frequencies²⁴. According to Lessig, this qualitative leap completely changes the fundamental right of intellectual property from an individual, personal right to the right of the cultural industry²⁵. Therefore, it is fair to say that among the negative consequences brought about by the excessive use of technology is, without a shadow of a doubt, the infringement of the right to property²⁶. Article 832 of the Civil Code reads as follows: 'property is the right to enjoy and dispose of things fully and exclusively, within the limits and in compliance with the obligations established by the legal system'. Thus, it is configured as the full and exclusive ownership over a given good. It is a right of full and exclusive ownership and does not merely refer to movable or immovable property but also extends to

²⁰PIETRANGELO M., *La società dell'informazione tra realtà e norma*, Giuffrè Editore, 2007.

²¹GAUDENZI A.S., *Intellectual Property, Industrial Law and Information Technology*, GRUPPO24 ORE, 2022.

²²UBERTAZZI LC., *Intellectual Property and Privacy*, *Il Foro Italiano*, 2014. ²³MAZZOLENI P., *Living in the Information Society*, Libreria CLUP, 2006. ²⁴RODOTA' S., *A Constitution for the Internet? - Politics of Law*, rivisteweb.it, 2010.

²⁵ROSSI G., *La proprietà caduta nella rete*, *Corriere della Sera*, 02/12/2004.

²⁶GHIDINI G. - CAVANI G., *Intellectual Property and Competition*, Zanichelli Editore, 2022.

those works that are the fruit of the genius²⁷. For years now, Italian and international jurisprudence has been coming to terms with the Internet. We are, in fact, faced with the generation of 'digital natives', i.e. those subjects who make abundant use of technology from their earliest years. They must be protected because there are many risks they may incur that they are unaware of. In addition, it appears that they do not perceive the exchange of certain information as unlawful and, therefore, stage certain behaviours unconscious of their unlawfulness. The doctrine has long wondered about the possible solutions to be adopted, coming to the conclusion that it would be advisable to limit those intangible and legally protected goods that are exposed and exploited on the net. It is possible that the presence of the Internet within a company, in fact, infringes intellectual and industrial property rights, sometimes also affecting the interests of others. It is no coincidence that the European Court of Justice intervened in 2019 with a ruling requiring platforms such as Facebook to constantly monitor, through special filters, the behaviour of their users so that they refrain from committing unlawful acts²⁸. So, for better or for worse, the Internet has really revolutionised our lives and the way we approach everyday life. Especially in the world of work, technological and digital transformations play a crucial role²⁹. A real revolution has been the digital transformation, i.e. the process that has fully replaced manual and traditional ways of working with the latest and most advanced digital techniques. Obviously, such a change within a company entails a modification of the entire organisational process. The digital transformation has strong roots dating back to the early 1990s when the mass media broadcast extensive advertising campaigns³⁰. Purchases were made physically in shops, but the digitisation process was beginning, and in 2000, it was social media and mobile devices that introduced new ways of communicating and doing business³¹.

. At the same time and to facilitate this process, new payment methods for

²⁷UBERTAZZI LC., Intellectual Property and Privacy, Il Foro Italiano, 2014.

²⁸BUFFARDI A., Futuri possibili: Formazione, innovazione, culture digitali, Egea, 2022.

²⁹FRANCESCHELLI V., Convergence: The "convergence" in telecommunications and copyright in the information society, Giuffrè Editore, 2009.

³⁰MOROZOV E., Internet will not save the world, Mondadori, 2014.

³¹PACCAGNELLA L., Open Access. Open Knowledge and the Information Society, Il Mulino, 2010.

shopping were introduced, such as PayPal, Venmo and Zell³². Undoubtedly, in a modern and technological age such as ours, online commerce and services have taken over, and companies are increasingly using huge amounts of data mined from social media and mobile devices with the intention of ensuring a better customer experience³³. Unfortunately, technological advances are subject to constant updates that put pressure on companies to adapt and thus digitise in order to survive, but, at the same time, it is confirmed that new technologies positively change not only the production process but also the products themselves and the relationships with customers and suppliers³⁴. In order for digital transformation to be successful, it is necessary for companies to follow some specific strategies in order to avoid unsuccessful situations for themselves and the market³⁵. First and foremost, an organisation must decide what it wants to achieve and what its objectives are before embarking on the path towards digital transformation. It is also important to be constantly updated on everything that can increase opportunities and benefits. It is then necessary to focus not only on the 'what' but also on the 'how' of each new endeavour and to embark on an agile journey that simplifies management by keeping an eye on the user experience and transforming business services³⁶.

2. ARTIFICIAL INTELLIGENCE BLOCKCHAIN AND SMART CONTRACTS

Smart contracts have the capacity to self-execute without the need for third parties and intermediaries to act as guarantors of execution. By translating contractual clauses into code and embedding them in hardware or software, they are able to self-enforce them. The minimisation, therefore, of intermediaries means that the main character of the smart contract is that the parties reach an agreement on contractual terms and timeframes by exploiting the logic of 'if-this - then that, i.e. if an assumption (this) occurs, then a result (that) follows. Author

³²DE MINICO G., *Internet. Regola e anarchia*, ARACNE Editrice S.r.l., 2012.

³³BUFFARDI A., *Futuri possibili: Formazione, innovazione, culture digitali*, Egea, 2022.

³⁴DEL RE C. - ROTINI F., *Brevetti e Proprietà Intellettuale-Manorico-Pratico*, Pacini Editore Srl, 2022.

³⁵BENTIVEGNA S., *Digital Inequalities. Le nuove forme di esclusione nella società dell'informazione*, Laterza, 2009.

³⁶GUIDOTTI E., *Internet e comunicazione. Per capire come cambia il modo di comunicare l'impresa con Internet*, Franco Angeli editore, 1997.

Nick Szabo defined smart contracts back in 1994 as computerised transaction protocols that execute the terms of a contract. In essence, the smart contract has the ability to enforce its terms and enter into execution without the support of an external party. In other words, the smart contract code is designed in such a way that it can be executed upon the occurrence of a certain condition. The re-evaluation of smart contracts came about following the advent of blockchain technology. In fact, the advent of this new technology, in its various declinations, has made the smart contract affair current and viable. Systems such as Ethereum³⁷, capable of interconnecting multiple computers in a shared system, enable different blockchain applications by harnessing the computational power of the network. In fact, the computing centre, by augmenting the consensus mechanism, guarantees the smart contract with respect to its execution. In such systems, the smart contract is contained and registered in all computers participating in the network, miles of computers acting as one according to the consensus mechanism. In essence, execution cannot be stopped or suspended unless this has been entered into and foreseen by the programmers.

Smart contracts cannot be traced back to a classical scheme of law, but they can be considered a means of executing a contract. That is, the negotiation agreement is assumed to be upstream of the smart contract. Thus, the incorporation of the clauses into the software, excluding human intervention, within the framework of a decentralised system, to all intents and purposes, makes breach of contract impossible. It is the network itself, due to its peculiarities, that guarantees the correct execution, as the smart contract is recorded on an electronic, decentralised, replicated and distributed register used to make transactions automatic. The Italian legislator with Art. 8-ter of the Simplification Decree of 2019, conversion law D.L. 135/2018³⁸ attempted to regulate the phenomenon by providing for the following points: 1) "*Distributed ledger-based technologies*"

³⁷Ethereum was born in 2013 and can be defined as a large shared computer according to the logic of distributed computing that replaces the distributed ledger, i.e. a real-world system in which all computers are connected, but the system is autonomous from the computers that make it up. This has binary functionality containing both the production of contracts and remuneration for users.

The revolution of such a system was the creation of a true single-state world computer guaranteed by the rules of consensus

³⁸Decree 135/2018 'Distributed ledger-based technologies and smart contracts', source Official Gazette

are defined as those IT technologies and protocols that use a shared, distributed, replicable, simultaneously accessible, architecturally decentralised ledger on a cryptographic basis, such as to allow the recording, validation, updating and storage of data both in plain text and further protected by encryption verifiable by each participant, not alterable and not modifiable. (2) A "smart contract" is defined as a computer programme that operates on distributed ledger technologies and whose execution automatically binds two or more parties on the basis of effects predefined by them. Smart contracts meet the requirement of being in writing upon computer identification of the parties concerned through a process having the requirements established by the Agency for Digital Italy by means of guidelines to be adopted within ninety days from the date of entry into force of the law converting this Decree. (3) The storage of an electronic document through the use of technologies based on distributed registers shall produce the legal effects of electronic time stamping referred to in Article 41 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.

Authoritative doctrine holds that the smart contract acquires the force of law pursuant to and for the purposes of Article 1372 of the Italian Civil Code only from the moment of its execution, thus paving the way for a '*tertium genus*' with respect to the formation of the contract³⁹, i.e. the conclusion by widespread validation, i.e. validation understood as a mechanism of consent that occurs through the widespread nodes of the blockchain. Now, we can distinguish between smart contracts depending on the concluding moment of the agreement, i.e. whether they are a mere act of execution with respect to a 'smart contract' agreement concluded and occurring outside the network or true contracts concluded 'in the network', as when these 'smart contracts' contain the fundamental elements of the contract, i.e. when the proposal reaches the offeree; this is the case brought by Art. 1336 concerning the public offer, concerning an offer containing the essential elements directed towards a conclusion, such

³⁹CERRATO S. , Traditional contracts, contract law and smart contracts, in Blockchain and Smart Contracts, edited by Raffaele BATTAGLINI, Marco GIORDANO, Giuffrè Francis Lefebvre, Milan, 2019, pp. 300-301.

Proposals would become binding if acceptance arrived at in the given form. If, on the one hand, the smart contract can be considered a free-form contract even though it meets the requirement of a written form due to the fact that it is a programme, the will and the form of the meeting of the same cannot be automated as this requires human intervention which is material through the affixing of a digital signature. A problem to be highlighted lies in the fact that the smart contract is a software program written in a machine language that is comprehensible only to those who are computer experts; therefore, from the point of view of protection, the party that does not know this language could fall into error. On this point, we consider Art. 1477 of the Civil Code to be applicable for the purposes of cancellation for a mistake in the aforementioned hypothesis. The smart contract is irrevocable from the moment it is entered into the blockchain that gives rise to its automatic execution; should issues of a pathological nature develop, remedies may already be contained in the programme, such as the Kill⁴⁰ function of Etehereum.

Blockchain, literally 'chain of blocks'⁴¹, represents a technological evolution that is challenging the world of law. Trying to give a definition, the word 'blockchain' means 'concatenated blocks' and it is possible to imagine it as a concatenation of blocks made up of a set of verifiable transactions, capable of linking different nodes, physically constituted by the servers of each participant in the network, which are used by the subjects to take part in the decision. Blocks are packets of data marked with a specific code called a hash that allows anyone to verify their authenticity. One of the fundamental characteristics of the blockchain is that it is comparable to a ledger in which every transaction is recorded in the system and cannot be changed, modified or tampered with in any way. In fact, to add a new block to the chain, there is a precise consensus protocol between these nodes. The blocks are concatenated because the hash of the previous block is included in the data packet of each block. Once all servers express the consensus, the new block is added and each node will update its copy without any

⁴⁰ The kill function is a self-destruct mechanism of the smart contract, which can only be activated by the node that created the smart contract.

⁴¹ GARAVIGLIA R., *Comparative Law and the Blockchain*, Hoepli Editore, 2021.

possibility of modifying the data once validated and entered⁴². Indeed, through this system, it is possible to manage and update data and information easily and quickly by exploiting the features of a computer network. New models of interaction are thus created, even avoiding, at least from a potential point of view, the use of banks, notaries, financial institutions and so on. The start was made with Bitcoin, which opened the digital blockchain revolution. The concatenation of blocks links several nodes, each of them containing the cryptographic code of the previous node⁴³ opening a chain linking previous and next.

The technology behind blockchain is based on a distributed system through which copies are made at different points in the network 'nodes'. However, each node is independent of the others while communicating and/or connecting with the others. The main features of the blockchain system are decentralisation and cryptography, the latter containing the algorithm and the key. The asymmetry of the encrypted system involves a public key and a private key, the former known to all those who have some form of interest in sending a message, while the private key is known only to the recipient who will use it to decrypt the message and read it. The cryptographic function that is used is the hash function, which is characterised by the fact that even the slightest modification of the message conveyed causes the alteration of the entire code string 'avalanche effect', so in such cases, the user immediately realises the tampering and alteration. Just think that a digital signature system uses precisely the hash function since the identifier is unique. Hence, it follows that, precisely because of its uniqueness, this function can be used to authenticate any document.

⁴²This approach is the result of the work carried out by Satoshi Nakamoto (whose real identity is still a mystery today), following the world economic and financial crisis of 2008 (S. NAKAMOTO, Bitcoin: a Peer-to-Peer Electronic Cash System). The publicity of this register is a reaction to the classic payment system and is linked to the trust placed - by the average user - in intermediaries, who are guilty of (maliciously or negligently) losing their guarantee function. Therefore, the concept of trust will change, and will pivot on a distributed public register, accessible and visible to all. Influential authors argue, then, that the Blockchain would represent "the first system, still the most widespread, of trustless payment" (F. SARZANA DI S. IPPOLITO, M. NICOTRA, Blockchain Law, Artificial Intelligence and IoT, Milan, 2018, 9).

⁴³F. SARZANA OF S. IPPOLITO, M. NICOTRA, Blockchain Law, Artificial Intelligence and IoT, Milan, 2018, 9).

We can distinguish 'permissionless' public and 'permission' private blockchain systems at this point. The code of public blockchains is, by definition, open source, and the blockchain is continuously modified automatically. In private blockchains, the source code and the database are the subject of intellectual property by the author. Depending on the number of participants in the Blockchain network and whether or not they can make decisions within it by 'consensus', systems can be distinguished. In the public network, the system is completely decentralised, and each of the nodes has a copy; a certain number of authorisations are required to make a change. It is emphasised that anonymity prevents any form of censorship as the public network is open to all, and the user, once consent has been obtained, adds a transaction to the registry, making the documents within a huge database immutable over time. Private networks, on the other hand, are centralised, managed by an organisation, and used by all those authorised to use them, such as companies, banks, etc. Distributed records become interesting for the business world through the consensus mechanism; however, the sheer size and importance of the business sacrifices decentralisation.

It is possible to divide the main areas of application of the Blockchain into three macro-areas:

- Internet of Value, i.e. those applications that are based on the exchange of value (cryptocurrencies, stablecoins and virtual currencies);
- Blockchain for business, by which we highlight those projects in which traditional business processes are replicated using Blockchain technologies;
- Decentralised web, which introduces new models of interaction, such as decentralised applications (DApp, short for Decentralised Applications), the world of NFT (short for Non-Fungible Token) and collectibles⁴⁴.

Today, more and more companies are making use of the techniques pioneered by Blockchain. Indeed, information systems, driven by the need for decentralisation

⁴⁴CIOLLI G., MAGGESI M., Blockchain, cryptocurrencies and smart contracts, Torrossa, 2023.

and cooperation, have adapted to centralised schemes and distributed models⁴⁵ and are widespread. In this respect, distributed object technologies and Distributed Object Computing (DOC) play an important role. There are two systems that are mainly considered: shared and distributed.

The former is configured when data and applications are centralised in a single processing core. Conversely, we have a distributed computing system when one of the following conditions occurs:

- applications are located on multiple processing points (distributed processing) and cooperate with each other;
- the information assets are unitary but distributed across various processing nodes (distributed database)⁴⁶.

In general terms, therefore, a distributed system consists of a set of logically independent applications that collaborate in the pursuit of common goals via a hardware and software communication infrastructure⁴⁷. Such communication, unlike in non-distributed systems, would exploit a message exchange system instead of calls. Characteristics of such systems are:

- resource sharing
- simultaneous processing
- scalability
- error detection
- transparency.

The smart contract is therefore an IT tool that autonomously governs certain events affecting the relationship between two or more parties on the basis of instructions decided by them, and takes shape precisely through the blockchain.

Thus, we can extol the progress and modernity represented by the new technologies that, with the help of the internet, have completely revolutionised in positive terms the way we approach and interact with society as a whole, as well

⁴⁵In fact, the processing of blockchain lifecycles is essential for the efficiency of a blockchain, which consists of four phases: creation, execution, consensus and validation.

⁴⁶CIOLLI G., MAGGESI M., Op. cit.

⁴⁷GARAVIGLIA R., Comparative Law and the Blockchain, Hoepli Editore, 2021.

as, at the corporate level, the organisational means, thus allowing for increased benefits and significant improvements in every respect, from production to external relations, technologies such as artificial intelligence (AI), blockchain and the Internet of Things (IoT) are converging to drive the next wave of digital revolution. The combination of the aforementioned advances with critical infrastructure (CI) can significantly help society by providing a better quality of life and boosting the nation's economy and productivity⁴⁸. Artificial intelligence (AI) and blockchain are two disruptive technologies that prove to be a powerful combination, capable of improving virtually any industry. Artificial intelligence research has come a long way, and many companies, organisations, and individuals have benefited greatly from machine learning services⁴⁹. Smart contracts are a technological innovation that, through blockchain technology, conduct transactions securely, quickly and with almost no risk of non-compliance. A smart contract is a computer code running on a blockchain that contains a set of rules under which the parties to the smart contract agree to communicate with each other. The interconnection of these technologies combined with the use of AI systems will, in the near future, allow for automated agents capable of proposing the conclusion of smart contracts and supervising their exact execution. It is assumed that AI-enabled and blockchain-enabled smart contracts will have a huge effect on the financial industry and digital trade in the future. This technological implementation poses a great challenge to the jurist in terms of identifying the operating dynamics relating to the completion of the contract and the manifestation of consent, as well as the consequences relating to non-performance or improper performance in the execution of the contract. Once again, a fundamental question arises as to whether domestic and European legislation is capable of dealing with the new technological phenomena with the tools that have matured so far or whether an ad hoc organic

⁴⁸Abdulova, E., Kalashnikov, A. *International Journal of Critical Infrastructure Protection* Volume 44 March 2024 Article number 100647.

⁴⁹PATIL A., ASAD S., conference proceedings " *International Conference on Circuits, Control, Communication and Computing, I4C 2022*", A Blockchain-based framework for creating and sharing machine learning models, Ramaiah Institute of Technology, Karnataka, Bangalore, India.

regulation as broad as possible is needed to deal with figures of damage resulting from the massive use of new technologies.

3. INTERNET SERVICE PROVIDER CONTRACTS

In today's digital ecosystem, the figure of the Internet Service Provider has assumed an increasingly important role, both for access to and operation of the Internet and for the promotion of economic growth in the digital economy, as reflected in the latest EU policy.

Over time, ISPs have assumed greater market power and are able to influence public opinion. In light of this evolution, the regulation of ISPs' liability for the dissemination of illegal content is one of the cornerstones of the regulation of their activity. In fact, illicit contributions, although generated and placed on the network by third parties, are visible and accessible to all, thanks to the spaces managed by intermediaries. Moreover, the activity of the Internet network is configured in such a way that, on the one hand, it is difficult to identify the creators and perpetrators of unlawful conduct, and on the other hand, the intermediary is the one who, through his activity of creating and managing spaces, makes it possible for unlawful acts to occur. Consequently, without the activity of intermediation, certain offences would not be possible.

The purpose of this article is, therefore, to retrace the most significant moments in the evolution of the liability of Internet intermediaries within the EU legal system and the Italian legal system and to identify the liability regime in the single digital market as regards content generated or disseminated by third parties. The main need is to balance the development of certain sectors of the economy and the proper exercise of freedom of expression with the need to prosecute the authors of certain illegal activities.

4. RESEARCH QUESTION

The emergence of new electronic tools that characterise modern society, increasingly oriented towards massive computerisation, has generated new problems that cannot leave the jurist indifferent. The globalisation and the diffusion of computer tools brings with it makes the Internet a tool that, on the one hand,

offers new and relevant opportunities, both socially and economically, but, on the other hand, requires a uniform regulation that, through the definition of common standards, is concerned with preventing the rights of third parties from being infringed by the use of new technologies. In fact, although the Internet can be considered an important tool in various spheres of life, the possibility of access to a global mass of recipients multiplies the circumstances in which damage can occur. The advent of the *new economy* has completely changed the liability scenario, creating not only new dangers but also new areas in which they can occur. Cyberspace is one of these and, having special characteristics requires special discipline. This sector requires the presence of subjects (providers) who, by providing their services within the information society, make the flow of data that make up websites materially possible. The provider is, therefore, the professional subject that offers services consisting of the transmission and/or storage of data and information of all kinds (commercial and otherwise) by users. According to these preliminary considerations, it is therefore necessary to ask the following question: according to European and national legislation, are *ISPs (Internet Service Providers)* liable for illegal activities and content placed on the web by third parties? Can distributed systems be a possible solution to the need for data certainty in civil law relations? Can smart contracts be considered real contracts? And whether the frequency of regulatory response in Italy is sufficient to cope with technological change.

5. ANALYSIS OF REGULATORY RESPONSE FREQUENCY VERSUS TECHNOLOGY IMPLEMENTATION IN ITALY

According to the DESI index (European Commission's digitisation index), Italy ranks 8th among the 27 EU countries by the year 2022⁵⁰. In fact, it seems to be gaining ground both because of the substantial investments aimed at closing the gap with other EU countries and because of the presence of a strong industrial

⁵⁰European Commission "Digitisation index of the economy and society 2022 Italy" section 1.3 of the thematic chapters of DESI 2022, in which the twelve development indexes of the twenty-seven EU countries are reported in which Italy ranks 18th, obtaining 49.3 points on the scores set by the indicators for 2022; Shaping Europe's digital future in <https://digital-strategy.ec.europa.eu>

base and research communities in key sectors such as artificial intelligence, high-performance computing and quantum computing. However, regulatory production in the sector, as will be seen above, is travelling at a slower pace than the acceleration of technological development. On the basis of the twelve DESI indicators, we can see that half of Italian citizens lack basic digital skills, while 60 per cent of small and medium-sized Italian companies have only achieved a basic level of digital skills. From this data, we can deduce that the absence of technological skills and a widespread digital culture, which sees a large part of knowledge concentrated in the hands of large groups, as well as the application of the same in terms of services, represents and will represent for the future, if no regulatory corrective action is taken, an area of social inequity linked to socio-economic control. As far as human capital is concerned, Italy ranks only 25th out of 27 EU countries. In fact, only 46 % of people in this range possess basic digital skills, which is below the EU average of 54 %. The gap with the EU average is narrower when it comes to people possessing digital skills 'above' basic skills (23 % in Italy compared to 26 % in the EU). If one takes into account that the 'civilisation' development linked to the production of legislation on technology is the child of a reform package adopted only in this period, aimed at the implementation of existing digital infrastructures, one can understand how the Italian regulatory system, without prejudice to the exegetic efforts of jurisprudence, is completely obsolete, inadequate and out of line with the European average. Italy ranks 8th in the EU in terms of digital technology integration. The use of big data is quite low (it is used by 9 % of Italian companies compared to an EU average of 14 %), as is the use of artificial intelligence-based technologies (6 % of Italian companies, while the EU average is 8 %). With the Decree of 6 December 2021 of the Ministry of Economic Development, the national fund for AI, blockchain and the Internet of Things was activated, while AgID, Infratel (MISE), in which we find Poste Italiane, Sogei and 20 other public entities (including universities) created the Italian Blockchain Service Infrastructure (IBSI) in 2021, in order to define national use cases, enabled by distributed ledger-based technologies. With respect to technology integration, the DESI index for 2022 ranks Italy 8th with a score of

40.7. In Italy, from 13 December 2022 to 13 December 2023, 83 laws were passed, of which 40 laws converted decree-laws and 42 other ordinary laws. With respect to this figure, it should be noted that only 6% of the regulatory production in this period concerned economic development (equal to 5 measures), while the environment, land and infrastructure sector produced 9% of the regulatory incidence, equal to 8 regulatory acts⁵¹ on a boundless subject. In the analysed period, 36 legislative decrees were published in the 'Official Journal'; in 24 cases, they were legislative decrees transposing EU legislation; of these, 8.3 % consisting of 3 measures were dedicated to economic development. Overall, 33.3 % of the range involved the implementation of state laws, while

66.7 % concerned the implementation of European law. In comparison with previous years, in the period from 23 March 2018 to 10 August 2021, 213 laws were produced, 5% of which were dedicated to economic development with 10 measures and 6% to the environment, land and infrastructure sector with a total of 13 measures, 69% of which were related to the implementation of European legislation and 31% to national legislation. It is precisely the phase of technological integration that makes the difference, i.e. the use of multiple 'innovative' instruments, even those born with different purposes that meet and implement each other. The target that the EU proposes of 20% in digital transition as far as Italy is concerned does not seem to be a good match, as the rate of growth and technological increment travels at a speed that is certainly greater than the process of normative production, not only by the state but also at a European level. Smart contracts, themselves technological tools, encounter the technology of distributed blockchain systems that need the tools and infrastructures of Internet service providers to function. The decentralised, encrypted and self-executing nature of blockchain technology applications would seem to operate in parallel with classical legal institutions, which are certainly inadequate; however, this system entails important questions related to legal liability for damage, which is a constant with respect to the development of new technologies and the applicable jurisdiction, in addition to posing serious

⁵¹ Servizio studi Camera dei Deputati, XIX legislatura, 'la produzione normativa: cifre e caratteristiche', 13.12.2023;

questions related to consumer protection. In fact, 'ledgers' without legal personality become the focus of the reasoning, they are entrusted with responsibilities and obligations, which are not sustainable under the current regulatory systems, sacrificing transparency, opening the door to unenforceable justice. The distribution of consensus on the blockchain platform does not make the technology-neutral; in fact, the need for an organic and cross-border formation capable of 'nonetheless' not hindering the evolution and progress of the technology has been expressed in European circles.

6. EUROPEAN ISP REGULATION

ISP liability has recently been the subject of attention not only in doctrine but also in case law. The United States was the first to address the various issues related to network use and the role and responsibilities of the Internet provider. The first piece of legislation that dealt with this issue dates back to 1996⁵², known as the *Communications Decency Act*, which was intended to curb the social concern that had emerged as a result of the evolution and mass distribution of the Internet, such as defamation and the dissemination of obscene material. Apps were created in which it is possible to publish or simply consult sexual images and reproductions. But pornography is not a game; it constitutes a real crime. In an age where everything happens at the click of a button, we are led to believe that every action is lawful, without limits or controls and without respect for the privacy and dignity of others. Pornography is a crime punishable under Article 600 quarter of the Criminal Code, a provision that incriminates and punishes anyone who 'outside the hypotheses provided for in Article 600 ter of the Criminal Code, knowingly procures or possesses pornographic material made using minors under the age of eighteen years, with imprisonment of up to three years and a fine of no less than EUR 1,549.00'⁵³. Various legislative interventions have been made to combat and punish sexual offences. The Court of Cassation, in January 2017, ruled that 'the possession of child pornographic

⁵²GATTEI C., Considerazioni sulla responsabilità dell'internet provider, www.interlex.it, 1998

⁵³RAZZANTE R., Handbook of information and communication law, CEDAM, 2002.

material stored in the cache memory of a personal computer is a crime.⁵⁴ A recent legislative intervention, in January 2022, aimed to remedy sexual violence and pornography offences, particularly online, by introducing important novelties in this regard and introducing the new criminal hypothesis of intentional access to sites containing pornographic material⁵⁵. In addition, a recent legislative intervention, in January 2022, set out to remedy sexual violence and pornography offences, particularly online, by introducing important innovations in this regard and introducing the new criminal hypothesis of intentional access to sites containing pornographic material⁵⁶. Right from the early years of the development of the Internet, it was realised that freedom of expression risked degenerating into its most deleterious meaning, i.e. into defamation and the dissemination of pornographic material. The *Communications Decency Act* almost absolutely sanctioned the non-liability of Internet service providers in relation to the aforementioned offences. It also gave Internet service providers enormous censorship power, as they could decide for themselves what content was defamatory and obscene and whether it should be removed. However, the *Communications Decency Act* was soon accused of presenting various profiles of unconstitutionality and of giving *Internet Service Providers* excessive discretionary powers⁵⁷. Although the above-mentioned act was repealed rather abruptly, the principle of non-liability essentially remained in force. The approach and procedure followed by the United States was taken up in a European Union Directive No. 2031 of 2000⁵⁸, aimed at regulating electronic commerce. In particular, Articles 12, 13, and 14 distinguish between the activities of mere conduit, caching, and hosting providers, while in Article 15 of Directive 2000/31/EC, the EU legislator states that the provider has no general obligation to monitor the information, just as there is no obligation to search for

⁵⁴Cass. Sec. III, 11 January 2017.

⁵⁵Art. 20(1)(a), Law 238 of 13/12/2021.

⁵⁶METITIERI F., *Il grande inganno del web 2.0*, Editori Laterza, 2021.

⁵⁷MAGLI S. - SPOLIDORO M.S., *The liability of Internet operators: domestic and international profiles*, Information and Computer Law, 1997.

⁵⁸Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') - <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000L0031&from=ET>

facts or circumstances from which the unlawful activities may take place. Consequently, the provider is exempt from liability for offences committed through the use of the network. In particular, the provider is not liable for failing to take repressive measures if other users have committed infringements⁵⁹. The adoption of this regime allowed a balancing of opposing interests: on the one hand, favouring technological progress and the development of e-commerce, and on the other hand, prosecuting the commission of offences via the Internet. The EU directive of 2000 undoubtedly encouraged entrepreneurs who freely provided third parties with access to online services, which they would not have done if they had been burdened with liability for any torts committed by third parties⁶⁰. The European Court of Justice has intervened several times on ISP liability. In recent years, the figure of Internet providers has changed profoundly for a number of reasons: firstly, they have grown in size, becoming large and structured organisations; secondly, they are capable of indexing and filtering the content placed on the network by third parties. Consequently, the provider has taken on an 'active' connotation⁶¹, making a new regulation of the subject indispensable. These calls for a review of the provider's liability regime have necessitated intervention by the European Commission on several occasions⁶², making it necessary to clarify the role played by platforms in copyright matters.

With a renewed awareness of the new requirements in this area, the Commission, on 14 September 2016, presented a proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market⁶³. The proposal does not provide for an overhaul of the liability regime of the host provider but establishes that if intermediaries play an active role in uploading content, or in the optimisation or promotion of the offer, they may not avail themselves of the exemption clause from liability, provided for in Article 14 of

⁵⁹TOSI E., *Private computer and internet law: assets, contracts, responsibilities*, Giuffrè, 2006.

⁶⁰Montagnani M.L., *Illegal content and liability of intermediaries*, EGEA, Milan, 2018.

⁶¹MONTAGNANI M.L., *Illegal content and liability of intermediaries*, EGEA, 2018

⁶²On the occasion of the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Towards a modern and more European copyright regulatory framework*, 9 December 2015 COM (2015)626 final, as well as on the occasion of the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Online platforms and the Single Market. Opportunities and challenges for Europe*, 25 May 2016 COM (2016) 288 final.

⁶³RAZZANTE R., *Handbook of information and communication law*, CEDAM, 2002.

Directive No. 31 of 2000 is useful to protect only intermediaries who play a passive and technical role. This led to the introduction of a new EU Directive 2019/790 that intervened to regulate copyright and digital single markets. In particular, this directive outlines a new figure of a *hosting provider who plays an active role* and incurs liability if they do not merely perform a service activity but intervene to give public access to works or material that is protected by copyright⁶⁴. In such cases, the provider is obliged to enter into licensing agreements with the rightsholders⁶⁵ in order not to incur liability since the exemption in Article 14 of Directive 2000/31/EC⁶⁶ does not apply. In December 2020, the Commission presented a new proposal for a regulation, entitled *Digital Service Act*, a regulation regulating online platforms and digital services, with the aim of amending the contents of Directive 31/2000, which is no longer in line with the technological development that has taken place over the last twenty years. The new regulation emphasises the liability of *Internet Service Providers*. The *Digital Service Act* also reaffirms that ISPs are exempt from liability for offences committed by third parties on the platform managed by them, except in the case where, despite being aware of it, they have not acted promptly to prohibit access to the unlawful content or to remove content already present on the network⁶⁷. The ISP is liable for offences committed on its platform (even if it is not aware of them and has not acted actively) if it has direct control over the users who interact on the platform or if it operates a platform that allows online users to conclude distance contracts⁶⁸.

7. ISP REGULATION IN ITALY

⁶⁴MONTI A., Uno spettro si aggira per l'Europa: la responsabilità del provider, www.interlex.it, 2000

⁶⁵Recital 38

<https://eurlex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:32019L0790&from=RO>

⁶⁶RAZZANTE R., Handbook of information and communication law, CEDAM, 2002

⁶⁷DAVINI L., *The New Rules of the Digital Service Act*, Mantelli Davini, Avvocati Associati, International Contract Lawyers, 30.03.2021. <https://imantelli.eu/>

⁶⁸GOGLIA L., BURA A., THIEM T., *Copyright in the Digital Single Market*, Giappichelli, 2022

Prior to the entry into force of Legislative Decree No 70 of 9 April 2003⁶⁹, which transposed the European directive on e-commerce, the ISP's liability was brought under Article 2043 of the Civil Code. Consequently, in line with the principles governing contributory negligence of others, the ISP could only be held liable for the action carried out by its user if it had contributed to causing the damage, in turn by engaging in active or omissive, intentional or negligent conduct⁷⁰. It was only with the entry into force of Legislative Decree No. 70 of 2003 that national legislation gave way to the principles codified at the European level. The decree regulates the liability of the provider in Articles 14, 15, 16 and

17. In particular, the first three articles regulate three types of Internet providers: Article 14, the mere *conduit*, i.e. the activity of simply transporting information (email providers and telecommunications companies); Article 15, the *caching provider* (such as *Google search*), where the provider transmits the information entered by the recipient of the service and temporarily stores the data; Article 16 the hosting provider (eBay, Facebook, YouTube). Article 17 is entitled 'absence of a general obligation to monitor'⁷¹. The main difference between the EU directive and the national directive concerns the liability for the services provided by the host provider, which is governed by Articles 16(1)(b) and 14(1)(b). In particular, the national rule establishes that the provider must take action for those facts and circumstances that make the illegality of the conduct evident only when there is a communication from the competent administrative and judicial authorities, while the Community rule requires the provider to act immediately when it has become aware of the illegality⁷². Consequently, the rule of domestic law limits the obligation of the ISP to act, making it conditional on being informed by the administrative or judicial authorities, whereas the Community rule provides for an obligation to act whenever the communication comes from a person who assumes that his or her rights have been infringed⁷³. In

⁶⁹D. Legislative Decree No 70/2003, 'Implementation of Directive 2000/31/EC on certain legal aspects of information society services in the internal market, with particular reference to electronic commerce', <https://www.camera.it/parlam/leggi/deleghe/03070dl.htm>

⁷⁰RISTUCCIA R. - TUFARELLI L., *La natura giuridica di internet e le responsabilità del provider*, www.interlex.it, 1997.

⁷¹DE CATA M., *La responsabilità civile dell'internet service provider*, Giuffrè, 2010.

⁷²TOSI E., *Private computer and internet law: assets, contracts, responsibilities*, Giuffrè, 2006.

⁷³TROIANO O., *The enterprise of content, host and access providing*, in AIDA, 2007, p. 355 ff.

practice, however, this difference has appeared very slight since case law has repeatedly intervened on this point⁷⁴, affirming that, although it is not possible to invoke a general surveillance obligation on the part of the host provider, prohibited by Article 17 of Legislative Decree No. 70/2003, the latter is in any case required to remove unlawful content, after the complaint by the interested party, without having to wait for any request or communication from the competent administrative or judicial authorities. An example can be given by the 'Tiziana Cantone' case, a young woman who committed suicide due to the disclosure on social networks of images and videos that portrayed her in intimate moments with a man. The Court of Naples ordered Facebook to remove certain links and URLs immediately following the victim's complaint but, at the same time, rejected the defendant's request to prevent the posting of similar material. Over the years, various rulings have been made on this subject. In 2012, Facebook was taken to court by the Mediaset group and condemned for content published by third parties on the platform despite the fact that the social network is considered a passive host provider. Specifically, in a lawsuit before the Court of Rome, RTI S.p.A. and Ms Valentina Ponzzone, the singer of a cartoon theme song, sued Facebook Ireland Limited, which had ridiculed Ms Ponzzone by creating a page on the same social. Not only had the actress been offended by unsuitable and disrespectful comments, but at the same time, pictures and videos of the cartoon series had been published without authorisation. Despite several warnings, the removal of the above-mentioned took place only two years after reminders. The liability action brought by the plaintiffs was upheld because, while it is true that there are rights to freedom and manifest one's thoughts, these must in no way infringe the rights of the individual⁷⁵. In this circumstance, it emerged that Directive No. 31/2000 and the corresponding implementing decree No. 70/2003 are inadequate to regulate social platforms that are constantly undergoing a process of transformation. If, on the one hand, the legislator imposes liability for content published by third parties, at the same time it excludes the existence of a prior control obligation that falls on the provider. In

⁷⁴See Order of the Court of Milan of 5 September 2013 as well as Court of Rome 27 April 2016, no. 8437, in De Jure.

⁷⁵GAMBINI M., Le responsabilità civile dell'internet service provider, ESI, 2006.

spite of the various case law interventions, doctrine and jurisprudence continue to question whether or not to impute criminal and/or civil liability to ISPs due to the unlawful acts carried out by those who use their services⁷⁶. As stated above, in Italy, the liability regime applicable to ISPs is governed by Articles 14, 15, 16, and 17 of Legislative Decree 70/2003, implementing Directive 2000/31/EC on certain legal aspects of information society services. Specifically, referring to a criminal law point of view, we note that in doctrine, there are two models of Internet Provider liability⁷⁷. The first is inspired by the concurrence of persons between the person who puts the criminal material on the network and the Internet Provider himself. The second model, on the other hand, focuses on the liability of the Internet Provider, for which it would be sufficient to have demonstrated the Provider's failure to exercise control, pursuant to Article 40, cpv, of the Criminal Code, in order to impute the offence to the person in question.

CONCLUSIONS

A single technological breakthrough, or its advancement in a specific sector, should not be considered an isolated phenomenon but rather part of a broad and diverse ecosystem where all components interact. In fact, European indicators aimed at crystallising and measuring technological and digital advancement take this very fact into account. If, on the one hand, a country's regulatory output and frequency of regulatory production cannot be an evaluative element from a merely or exclusively quantitative point of view, on the other hand, it represents a fundamental datum for understanding the strength of reaction and the speed of intervention in regulating new and pervasive social phenomena.

⁷⁶BUGIOLACCHI L., Principles and open questions on the Internet Provider's non-contractual liability. *Una sintesi di diritto comparato*, in *Diritto dell'informazione dell'informatica*, 2000.

⁷⁷TROIANO O., The enterprise of content, host and access providing, in *AIDA*, 2007.

The increasing relevance and power that online platforms are gaining has led to their dominance in the field of the dissemination of thought and freedom of expression. Over the past decades, both the Court of Justice of the European Union and regional courts have repeatedly ruled on the issue of ISP liability. The courts have tried to strike a fair balance between the rights of online platform owners and rights holders. This is a delicate matter: if, on the one hand, it is essential to curb offences committed by means of the network, overcoming the general regime of no direct liability in the event of violations attributable to users or third parties, on the other hand imposing on intermediaries an activity of filtering and selection of content, under the threat of a sanction, would lead to an increase in management costs and an inevitable reduction of online platforms, so as not to incur the risk of liability. The risk would be to attribute censorship functions to providers that would be incompatible with the ordinary business of providing services. Blockchain platforms not being covered by a legal status become a field of inexigibility with respect to the obligation arising from the annotation of smart contracts on the ledger, and the protection of damages, in terms of imputability for damage, gets stuck in the shallows of the legislative vacuum, often attracted to the vis attractive of distant jurisdictions.