Journal of Law, Market & Innovation

ISSUE 1/2024

Journal of Law, Market & Innovation

1/2024

Editors: ***Riccardo de Caria – Lorenza Mola - Cristina Poncibò***

Journal of Law, Market & Innovation
Vol. 3 - Issue 1 - 2024
ISSN 2785-7867
Journal of Law, Market & Innovation
Editors-in-Chief:
Riccardo de Caria
Cristina Poncibò
Lorenza Mola (for the trade law issue)
email: editors.jlmi@iuse.it


TABLE OF CONTENTS

Fabrizio Esposito[*]

INNOVATION LETTER

PRICE PERSONALISATION: WALKING THE NOT-SO-BLURRIED LINE BETWEEN INNOVATION AND EXPLOITATION

JEL CLASSIFICATION: K12, K30

1 A Spooky Story

A few years back, I got a nasty bronchitis: for over a week, I could barely leave my bed to reach the sofa. In essence, my main occupation was coughing; and it was quite tiresome, too. The ideal scenario for binge-watching. Which is what I did. Soon, I had watched all my Netflix watchlist, even after having refilled it; twice. Next, I watched all the episodes of The Real Ghostbusters cartoons I could find on YouTube.

You see, I am a 'moderate' *Ghostbusters* fan. Why am I telling you this? Because I used my YouTube account, meaning that YouTube collected the information that in my early 30s, I watched *The Real Ghostbusters* for about 10 hours a day for several days. It does not take great intelligence (artificial or biological) to conclude that I have a 'moderate' preference for *Ghostbusters*.

If YouTube knows it, well, probably everyone in marketing knows it, thanks to data brokering. (You see, back then, I was an 'accept all cookies' kind of guy.) What can be

[*] Ph.D., LL.M. (EUI). Assistant Professor of Law, Universidade Nova de Lisboa, NOVA School of Law and CEDIS (Centre for Research on Law and Society). E-mail: fabrizio.esposito@novalaw.unl.pt. The author wishes to thank Dr Marco Giraudo for the kind invitation and encouragement to write this innovation letter.

done with this information? Consider these two alternatives that illustrate of the difference between innovative and exploitative uses of price personalisation:

1. When *Ghostbusters: Legacy* came out on streaming, I could have been offered extra content for a hefty price
2. A content-sharing platform offers me to rent or 'buy' *Ghostbuster: Legacy* with my account for 50 cents more than my wife, who is not a *Ghostbusters* fan

In this Innovation Letter, I will explain that, even if the first example includes a high price request and the second only a small one, the first should count as innovation, while the second should be considered exploitative. What do these examples have in common? They are both forms of economic discrimination. The first is an instance of versioning; the second is a form of price personalisation.

Section 2 articulates why I see no critical issue in the first case, but plenty thereof in the second one. Then, Section 3 draws attention to the complexity the total welfare view of efficiency implies in the context. Section 4 sketches a regulatory framework to deal with the second case. Section 5 will conclude with some considerations derived from a project I am about to conclude concerning price personalisation.

This topic is worth an innovation letter because the first case is 'business as usual', while the second might become the new normal. Yet, I will argue that even if the second case is the granular version of what we experience nowadays, the fact we tolerate it in some cases does not mean we should allow its granular version that we expect to become widespread sooner or later.[1]

In sum, I intend to offer an account that distinguishes desirable uses of price personalisation that should count as innovative business practices from uses that are exploitative and should be treated as such.

2 Analysis: Distinguishing innovative and exploitative uses of price personalisation

2.1 The morality of versioning: pricy innovation, but only if you want it

Versioning is the practice of offering multiple versions of the same product or service, often with premium versions charging an amount that is clearly above their marginal cost. Business class tickets on airplanes are a good of this.

Suppose that, like me, you see the market mechanism as a means to maximise consumer welfare or, more precisely, to implement a rich notion of consumer

[1] Joseph Turow, *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power* (Yale University Press 2017).

sovereignty.[2] Why is versioning fine? After all, some consumers end up paying way more than what it costs to produce the good or service they enjoy. Surely, we can imagine idealistic scenarios where innovation attempts are not uncertain and where there are no fixed production costs. Probably, in said scenarios, versioning would deserve strict scrutiny.

However, in the world we live in, I find that the power to choose between the cheaper and more expensive versions of the same good or service is sufficiently respectful of consumers. Surely, there is a positional dimension in consumption that does not receive enough attention.[3] For example, cars have become increasingly big over the decades. This is an important social dimension of consumption, but one that has probably to do with consumer responsibility towards the environment and future generations.[4] Envy for passengers with larger seats and better food does not deserve moral attention.

In sum, versioning is normally acceptable. If this is the case, using my personal data to draw my attention to a deluxe version of the *Ghostbusters: Legacy* movie that is expensively priced seems fine.

2.2 The immorality of personalised surcharges: commodifying yourself and profiting from it

Like the example I gave at the beginning, a personalised surcharge is any price applied to someone higher than the price charged to someone else just because the trader has reason to believe that one consumer is willing to pay more than the other.

Of course, in many contexts where bargaining takes place, the price asked by a party is the starting point for negotiations. A commercial airing these days in Italy shows a couple looking for a house to buy that, before meeting the seller, reinforce the need to hide any belief, emotion, and so on to each other. But the house is so amazing they keep fainting in each room they enter. Very funny; it is just the most important financial commitment in their life, most probably.

Similarly, one is advised not to wear expensive clothing and accessories when visiting a flea market. In all these cases, the trader can use information about yourself you make available to them to increase the price.

---

[2] Fabrizio Esposito, *The Consumer Welfare Hypothesis in Law and Economics: Towards a Synthesis for the 21st Century* (Edward Elgar 2022); Fabrizio Esposito, *The Consumer Welfare Standard, Consumer Sovereignty, and Reciprocity: An Evolutionary Foundation for the Positive Economic Approach to Law That Actually Works* (SSRN 2023).
[3] Robert H Frank, *The Darwin Economy: Liberty, Competition, and the Common Good* (Princeton University Press 2011). See, more generally, Ugo Pagano and Massimiliano Vatiero, 'Positional Goods and Legal Orderings' in Alain Marciano, Giovanni Battista Ramello (eds), *Encyclopedia of Law and Economics* (Springer 2017) 1613-1618.
[4] For a recent discussion of the role of this concept in EU law, see Lucila de Almeida and Fabrizio Esposito, 'Consumers and the Green Transition Between Saying and Doing: Promising Consumer Empowerment while Restricting' [2023] Yearbook of European Law.

Why can't an online platform do the same, then?

For a few reasons, really. First, in a face-to-face negotiation, bargaining goes both ways. Online, this is not the case; you cannot make counteroffers to an online store. Second, the degree of granularity in the use of personal information against consumers in the digital environment reaches unprecedented levels of granularity. This is unsurprising since the transaction cost savings of using price tags in the digital environment are way lower online than in offline settings.

So, to see the problem with personalised surcharges, we need to identify an ideal theory setting (without all the complications of the real, imperfect world) to establish a benchmark, and then look at the normalisation of price personalisation against said benchmark.

Under ideal conditions, on every market, at the same time, consumers maximise the benefits they receive, under the sole constraints represented by their preferences, the cost-reflective (or natural[5]) price, and their initial endowment. Under these ideal conditions, traders do not manage to benefit from knowing how much consumers are willing to pay because traders are price-takers.[6]

When price personalisation is possible, traders are not price takers. It follows that any expansion of price personalisation practices should be welcomed with suspicion. This consideration helps explain why price personalisation has attracted so much scrutiny among legal academics in the absence of overwhelming evidence of the practice being diffused.

Be this as it may, sometimes price personalisation can be beneficial to consumers and is, therefore, welcome. This is in particular, the case when it allows consumers who cannot pay market prices to access the market thanks to a discount. Another situation is that in which traders can use personalise discounts to make their competitors' customer base more contestable – for example, Pepsi offers targeted discounts to Coca-Cola loyal consumers; in this way, competition is increased under conditions of quality differentiation.

Notably, in both these cases, price personalisation makes real markets closer to ideal ones: it gives access to the market to consumers who would access it under ideal conditions; it stimulates competition between partial substitutes (under ideal conditions, substitutes are perfect).

None of this happens in the example I gave above. In said example, the content platform has collected my data and then used them to extract more economic rents from me, giving me nothing in return. In said example, the pricing novelty is used to

[5] Gianni Vaggi, 'Natural Price', in *The New Palgrave Dictionary of Economics* (Palgrave Macmillan UK 2018).

[6] More extensively, Patrick Coen and Natalie Tieman, *The Economics of Online Personalised Pricing* (Office of Fair Trading 2013). <https://webarchive.nationalarchives.gov.uk/ukgwa/20140402154756/http:/oft.gov.uk/shared_oft/research/oft1488.pdf> accessed 18 March 2024.

commodify part of what makes me 'me', namely my idiosyncratic, childish(?) passion for *Ghostbusters*. This novelty does not perform a desirable social function and, therefore, does not deserve to be called innovation. The Chinese get it: they call said practice big data backstabbing or swindling;[7] once the practice is named like that, it is apparent that it is tough to defend it in the public sphere.

I see no moral reason that justifies the possibility of taking my preferences, commodifying them, and selling them back to be, tied with a product sold to me for a price higher than everybody else's. It is invasive and exploitative. It moves us further from the ideal conditions of perfect competition, rather than closer to them. Thus, it should be prohibited.

The only reason I see to tolerate the practice is that it would be so costly to detect it that the cure would be worse than the disease. But the debate has not reached this point yet. Also, it is quite likely that, with some effort, cheap enftech solutions will be found.[8] This is an innovation worth pursuing in the context of price personalisation and pricing policy more generally.

3 Focus: Total welfare and analytical complexity

The previous analysis is not widely shared. Why? Because I move from a conceptual framework where the interest of consumers is at the core of economic analysis.[9] This is not what most people do nowadays. It used to be different in the past. Nowadays, market efficiency is about total welfare.

The point is that much of the scholarship on price personalisation moves from a very 'pluralistic' normative framework where there is total welfare, fairness, equality, distributive justice, at least.[10] When that is the case, it is easy not to know where to draw the line. The result is a legal bubble,[11] caused by a mixture of normative complexity, empirical uncertainty[12] and interdisciplinary opacity.

[7] Stella Chen, 'Big Data Swindling' (China Media Project, 5 October 2021) <https://chinamediaproject.org/the_ccp_dictionary/big-data-swindling/> last access on 8 December 2023.
[8] Liz Coll and Christine Riefa, 'Exploring the Role of Technology in Consumer Law Enforcement' (2022) 34 Loyola Consumer Law Review 359.
[9] Esposito (n 2).
[10] See, for example, Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy 347 and Oren Bar-Gill, Cass R Sunstein and Inbal Talgam-Cohen, 'Algorithmic Harm in Consumer Markets' (2023) Harvard John M Olin Discussion Paper, No. 1091 <http://www.law.harvard.edu/programs/olin_center/papers/pdf/Bar-Gill_1091.pdf> accessed 18 March 2024.
[11] Marco Giraudo, 'On Legal Bubbles: Some Thoughts on Legal Shockwaves at the Core of the Digital Economy' (2022) 18 Journal of Institutional Economics 587.
[12] Cf Fabrizio Esposito, Mateusz Grochowski and Kimia Heidary, 'Price Personalization', in Kimia Heidary, Vanessa Mak and Gitta M Veldt (eds) *Empirics and Consumer Law in Changing Markets* (Edward Elgar forthcoming) surveying the findings of empirical legal studies on this topic and limits thereof.

When, instead, you move from an ideal theory where the core of the market mechanism is consumer welfare maximization, it is hard to see why traders should be allowed to extract rent from consumers. As simple as that.

If, for some reason, under special circumstances, traders think it is defensible to do so, legal systems offer them plenty of occasions during both the regulatory cycle and the enforcement process to explain themselves. And judges have multiple techniques at their disposal to allow for an exception.[13]

4 Action: A regulatory framework that may work

Suppose we have a sense of situations where price personalisation is desirable and of situations where it is not desirable. In that case, we can try to figure out a framework that allows for the former and prohibits or at least makes less likely the latter.[14]

In the European Union, I have argued elsewhere and at length that traders have a duty to offer a price not based on personal data, especially in those economic contexts where they could be tempted to offer personalized surcharges.[15] This duty is primarily derived from the GDPR.

Thus, the information duty about personalised prices could require traders to disclose said price in the form of a discount or a surcharge in comparison to this impersonal price. Especially if consumers have an easy way to opt out of the personalised offer, one of two things will happen: either consumers selfishly choose the lower price (which is fine by me), or traders will give consumers reasons to stay with the personalised price. In essence, price personalisation will look way closer to versioning. If traders convince consumers to pay more when paying less is possible via rational persuasion, then I see no problem. Just like I see no problem with voluntary tipping, which is also a form of price personalisation.

The only problem left is avoiding traders artificially increasing the impersonal price and then offering personalized discounts to everyone. When we get there, between the new provision about reference prices in the Price Indication Directive (Article 6a) and the long tradition of anti-usury laws, we will eventually find a way to ensure the integrity of the impersonal price. We just need to put our minds to it.

Some scholars derive from the possibility of artificially increasing the impersonal price to everyone that there is no point in intervening. This is nothing more than a textbook

[13] Luís Duarte d'Almeida, *Allowing for Exceptions: A Theory of Defences and Defeasibility in Law* (OUP 2015).
[14] Fabrizio Esposito, 'Making Personalised Prices Pro-Competitive and Pro-Consumers' (2020) Cahiers du CeDIE Working Papers, No 2020/02.
[15] Fabrizio Esposito, 'The GDPR Enshrines the Right to the Impersonal Price' (2022) 45 Computer Law & Security Review 105660.

application of the conservative move Albert Hirschman called the Futility Thesis: there is no point in trying to improve the outcome; the market will make your efforts moot.[16]

5 The forthcoming Cambridge Handbook on Algorithmic Price Personalisation and the Law[17]

The handbook includes chapters by leading scholars who have analysed price personalisation from a variety of perspectives, including moral, historical, marketing, economic, and data science. The core of legal analyses focuses on EU law, is then complemented by overviews of the Brazilian, Canadian, Chinese, Indian and US legal systems.

Two points are worth anticipating here: first, contrary to what much (but not all) law and economics scholarship would suggest (also in the book), one finds broad normative convergence between moral and economic analysis in the direction sketched in this innovation letter; second, contrary to the self-celebratory view that the European Union is the best regulator in the world,[18] the regulatory experience of the other jurisdictions surveyed in the handbook are rich in useful insights, also for the European legislator.

[16] Albert O Hirschman, *The Rhetoric of Reaction: Perversity, Futility, Jeopardy* (Harvard University Press 1991).
[17] Fabrizio Esposito and Mateusz Grochowski (eds), *The Cambridge Handbook on Algorithmic Price Personalization and the Law* (CUP forthcoming).
[18] Cf Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020).

Cristina Poncibò[*], *Andrea Gangemi*[**], *Giulio Stefano Ravot*[***]

BLOCKCHAIN JUSTICE:

Exploring Decentralising Dispute Resolution Across Borders

Abstract

It is well known that the *raison d'etre* of Distributed Ledger Technology (DLT) is to enable peer-to-peer transactions that do not require Trusted Third Parties (TTP). Commercial security is a major concern for users in this new era: intermediaries are increasingly seen as security holes and removed from protocols as a result of a growing desire to maintain control over transactions. The need for independence from TTPs has evolved into a counterculture that moves blockchainers away from central authority, the courts and the world as we know it.

To date, all existing online dispute resolution (ODR) processes in DLT and related tools such as smart contracts do not reflect the vision of blockchain as a counterculture. They exclusively use adjudicative methods involving one or more TTPs deciding via on-chain incentivised voting systems. This paper aims to discuss why non-adjudicative methods shall have a cultural priority over adjudicative ones, showing why they might be preferred by blockchainers due to risk management and distrust concerns. Furthermore, we introduce a prototype of a non-adjudicative ODR model ("Aspera") in which users can have total control over the outcome of the dispute in a TTP free environment.

JEL CLASSIFICATION: G32, K12, E51, K22, J52

SUMMARY

1 Introduction

Distributed Ledger Technologies (DLT) have evolved into something beyond a mere scientific innovation embodying an ideal: they represent a true independence movement[1], the beginning of what could be called the cultural revolution of blockchain enthusiasts. Auinger and Riedl pointed out that the blockchain and its applications such

[*] Professor of Comparative Private Law, Department of Law, University of Turin, Email: cristina.poncibo@unito.it.
[**] Postdoc Researcher, Department of mathematical Sciences, Politechnic of Turin, Email: andrea.gangemi@polito.it.
[***] Postdoc Researcher, Department of mathematical Sciences, Politechnic of Turin, Email: ravotg@tcd.ie.

[1] See Primavera De Filippi and Aron Wright, *Blockchain and the Law* (Harvard University Press 2018). See also Michelle Finck, *Blockchain Regulation and Governance in Europe* (CUP 2018). See also Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Harvard University Press 2018).

as Bitcoin are not pure technical systems[2]; rather, they are socio-technical ones. The idea that technology is not just a neutral tool, but something deeper, is not new. Heidegger argued that the essence of technology is by no means anything technological, but intended it as "the way of revealing"[3].

Back in 1997, eleven years before the release of the Bitcoin white paper, Davidson and Rees-Mogg, in their work "*The Sovereign Individual: How to Survive and Thrive During the Collapse of the Welfare State*" - recognised by many as a true premonition - wrote about a "revolution of power which is liberating individuals at the expense of the twentieth-century nation-state". Through a comparative analysis of the various economic-political transitions over centuries, they describe the rise of the so-called "fourth stage of human society" centred on the denationalisation of individuals and the consequent break from states and centralised powers[4].

Technological utopians might argue that 2008 was - in Heidegger's words - the "revelation" year; what seemed to be a futuristic novel finally became reality. The rise of Bitcoin unveiled a need that many perceived but few were aware of: to be virtually free from Trusted Third Parties (TTP). The possibility of moving from a central authority trust model to a new form of "trust-free"[5] autonomous governance has given rise to an ecosystem, a culture, or rather, a counter-culture: the realm of millennials and gen-Z, who live in the idea of being beyond the state and beyond the law, who organise and communicate via anonymous accounts on networks like Discord or Reddit and who feel a strong distrust towards the traditional approach of doing things. It is a new way that does not ask for permission, self-financing through Initial Coin Offerings (ICOs) without the need for anyone, creating decentralised Decentralised Autonomous Organisations (DAOs) that belong to everyone and no one simultaneously. What happens in the blockchain creates a lot of interest for those on the outside, while those on the inside do not consider what they say out of crypto. "The blockchain philosophy is not only an expression of technology, but also a clear political and libertarian vision"[6]. In this sense, from a purely legal perspective, the same ideology may also appear hostile to law as a mere product of state power[7].

---

[2] Andreas Auinger and René Riedl, 'Blockchain and trust: refuting some widely-held misconceptions' (Information Systems XXXIX International Conference, San Francisco, December 2018).

[3] 'Technology comes to presence in the realm where revealing and unconcealment take place, where aletheia, truth, happens'. See Martin Heidegger, *The Question Concerning Technology and Other Essays* (William Lovitt tr, Harper Torchbooks 1977).

[4] See James D Davidson and William Rees-Mogg, *The Sovereign Individual: How to Survive and Thrive during the Collapse of the Welfare State* (Simon & Schuster 1997).

[5] See Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike and Simon Malone, 'Blockchain the gateway to trust-free cryptographic transactions' (2016) in ECIS Proceedings <https://aisel.aisnet.org/ecis2016_rp/153/> accessed 14 March 2024.

[6] Cristina Poncibò, *Il Diritto Comparato e la Blockchain* (Memorie del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino, 14/2020, ESI 2020) 19.

[7] ibid. See also David Post and David R Johnson, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367. See also David G Post, 'Anarchy, State, and Internet: An Essay on Making Law in

In a nutshell, "blockchain is actually revolutionary because it makes the anarchist utopia a more realisable dream than has ever before been possible."[8] Specifically, "the founding principles of the crypto-anarchist movement focus on opposing and inevitably weakening state power and institutions, neglecting the existence of laws, except for those expressed and enforced by computer codes"[9]. Even if this movement remains vaporous since it has never really materialised except beyond the province of libertarian dystopias[10], it cannot be ignored by the careful eye of the legislator.

This exaltation of technology[11] indirectly opens up numerous necessary considerations on what are the correct practises of dispute resolution and doubts on what is the right course to take for decentralised justice[12]. Ast and Deffains have been pioneers in asking whether - on a cultural level - users can perceive decentralised justice as a fair method of resolving disputes[13]. The current re-enactment of the ideals of scientism[14] may change the traditional perception of Alternative Dispute Resolution (ADR) models. The way blockchainers see the world also influences the way they are willing to solve their problems. Chase, in his masterpiece "*Law, Culture, and Ritual: Disputing Systems in Cross-Cultural Context*", presented empirical evidence on a deep and reflexive connection between culture and disputing processes. He shows how disputing practises mirror society: the way in which conflicts are resolved influences and changes in relation to the fundamental beliefs, values and symbols of the specific cultural context in which they operate. He directly addresses policymakers suggesting that "any proposal to borrow procedures from another society should prompt a cultural inquiry"[15].

In the following pages we will argue that the above-mentioned "cultural inquiry" has never been investigated before and that the current landscape of blockchain dispute resolution processes does not act in accordance with the cardinal principles of this technology and its related socio-technical system.

Cyberspace' [1995] Journal of Online Law <www.temple.edu/lawschool/dpost/Anarchy.html> accessed 14 March 2024.

[8] Brendan Markey-Towler, 'Anarchy, Blockchain and Utopia: A theory of political-socioeconomic systems organised using Blockchain' (2018) 1(1) The Journal of the British Blockchain Association 13.

[9] Poncibò (n 6) 18.

[10] Pietro Ortolani, 'The impact of blockchain technologies and smart contracts on dispute resolution: arbitration and court litigation at the crossroads' (2019) 24(2) Uniform Law Review 430, 432.

[11] Poncibò (n 6) 20.

[12] See Luis Bergolla, Karen Seif and Can Eken, 'Kleros: A Socio-Legal Case Study Of Decentralized Justice & Blockchain Arbitration' (2021) 37(1) Ohio State Journal on Dispute Resolution. See also Amy J Schmitz and Colin Rule, 'Online Dispute Resolution for Smart Contracts' (2019) 2 Journal of Dispute Resolution 103.

[13] See Federico Ast and Bruno Deffains, 'When Online Dispute Resolution Meets Blockchain: The Birth of Decentralized Justice' [2021] Stanford Journal of Blockchain Law & Policy <https://stanford-jblp.pubpub.org/pub/birth-of-decentralized-justice> accessed 15 March 2024.

[14] 'Scientism is the particular intellectual attitude of those who believe that the only valid knowledge is the physical and experimental sciences, and therefore devalue any other form of knowledge that does not accept the methods of these sciences' See Poncibò (n 6) 20. See also De Ridder, Rik Peels and René Van Woudenberg, *Scientism: Prospects and Problems* (OUP 2020).

[15] Oscar G Chase, *Law, Culture, and Ritual: Disputing Systems in Cross-Cultural Context* (New York University Press 2005) 48.

Section 2) will analyse how this cultural revolution of blockchain enthusiasts plays a primary role in the choice of the most appropriate Online Dispute Resolution (ODR) system, arguing that non-adjudicative methods have a cultural priority over adjudicative ones as they might be preferred by users for commercial security concerns. Section 3) will present the private companies currently operating in the smart contract dispute resolution market and the reflections proposed by the existing literature on on-chain incentivised voting systems. Finally, Section 4) will propose an alternative to the adjudicative methods for smart contract disputes: Aspera Anonymous Dispute Resolution[16].

2 Independence movement and non-adjudicative methods

Adjudicative methods are not suitable for a world marked by distrust of third-parties and are not a reflection of a counterculture that is distancing from the central authority day by day. Considering that users do not want to be dependent on the control of TTPs (such as banks) during their transactions, with a little creative effort it can be argued that they are probably not inclined to entrust a decision on a dispute arising from the same transaction to another third-party. With non-adjudicative methods there will not be an arbiter nor a judge as a decision-maker, which means blockchainers can keep their transaction completely decentralized even in the event of a dispute.

All existing dispute resolution processes in DLT and related tools such as smart contracts are exclusively adjudicative. This approach does not fit with the ideals of decentralization and independence from third-parties as the decision-making power always remains in the hands of one or more TTPs.

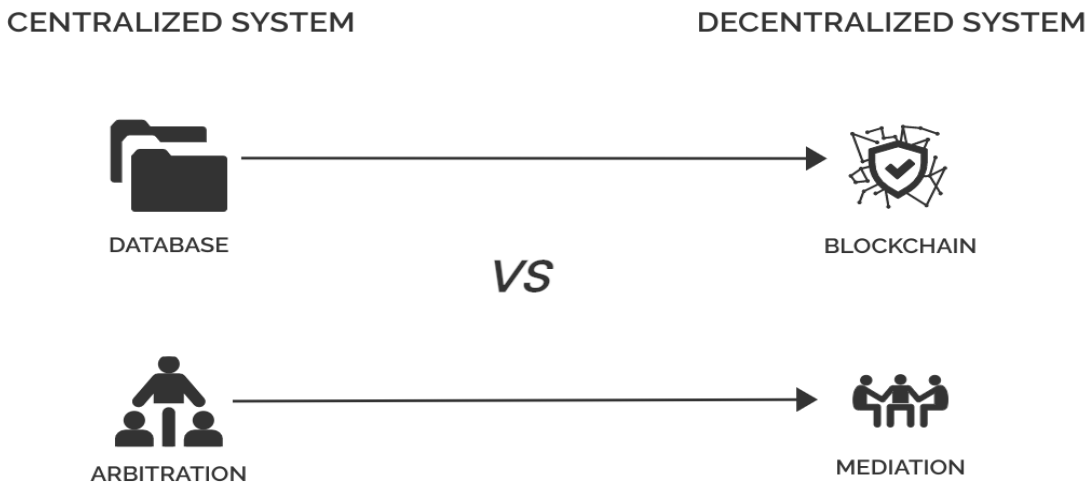
We already know that these specific target users do not want to be controlled. For this reason, the possibility to have total control over the outcome of the process and the possibility to manage their disputes independently and autonomously without intrusion of external decision-makers could be the success factors for the widespread adoption of amicable dispute resolution practices such as mediation in this specific socio-technical system.

Although a third-party will always be needed to maintain the rule of law, there are many reasons to argue that non-adjudicative methods deserve to be available as they might be preferred by users for concerns of risk management and distrust.

The cultural priority of non-adjudicative methods is represented in the following figure by comparing the two most currently used ADR instruments, namely mediation and arbitration:

[16] Aspera Anonymous Dispute Resolution. Available at <https://iris.polito.it/handle/11583/2949291>.

FIGURE 1. Parallelism between centralised and decentralised ADR instruments



It is well known that the database represents a centralised system, whereas the blockchain reflects the users' need for decentralisation. The same parallelism can be promoted by comparing adjudicative and non-adjudicative approaches. Arbitration through TTP is clearly a centralised system: an arbiter making a binding decision on the dispute is as close as one can get to the idea of a third-party hostile to blockchain users. In contrast, mediation fits perfectly with the need for decentralisation as it does not involve TTP, leaving decision-making power to the parties and implicitly granting them the full control they have long desired.

FIGURE 2. Differences between the judicial process and the main ADR instruments[17]

CATEGORY	JUDICIAL PROCESS	ARBITRATION	MEDIATION
Speed	Slower/ long-drawn process.	Relatively faster, Time-bound process.	Speedy resolution.
Costs	Increased litigation costs for longer durations in addition to Court fees.	Reduced costs as time bound.	Relatively inexpensive
Control over Costs	Limited as Court fees determined by Rules.	Fees of arbitrators can be pre-determined by parties.	Court-fee returnable, parties can decide fees of mediator.
Appointment of decision-making authority.	No control of parties-only judicial officers.	Experts from specific field can be appointed by the parties, with pre-determination of fees..	Parties can appoint mediator of choice.
Procedure for conduct of proceedings	Settled as per law.	Parties have authority to decide.	As per parties' convenience, not settled.
Evidence and Submissions	As per the law of evidence and CPC.	Parties can determine their own procedure.	Not bound by rules of evidence-flexible.
Forum Selection	Beyond control of parties.	Parties can exclude/ limit or confer jurisdiction on forum of choice.	Mediator is appointed on selection by the parties.
Privacy	Public proceedings.	Proceedings held in private.	Proceedings in private.
Appeal	Decision is appealable, as a matter of right.	Very limited grounds for appeal.	Settlement acceptable to both the parties is final and is not appealable.

The blockchain ideal is projecting us into a market of the future in which users increasingly want to be at the centre of their own transaction and want as much control over it as possible, without having to delegate decision-making, validation or control powers to anyone else. Specifically, Nick Szabo, in his famous *"Trusted Third Parties are Security Holes"*, argues that "a TTP that must be trusted by all users of a protocol becomes an arbiter"[18]; he also claims that the use of a third-party model "creates a bottleneck which imposes continuing high costs and risks on the end user"[19].

An idea of technological individualism that could oxymoronically create in users a communitarian spirit focused on the common enemy, the intermediaries, is slowly taking shape. This is not something new, but a historical prediction from the past; according to Chase, mediation emerged thanks to a decisive influence of the social context evocative of Woodstock and Haight-Ashbury in which traditional attitudes and authorities were challenged and shaken[20]. The concerns of anti-authoritarianism and self-actualisation reflected in the idea of "power to the people" of those years are not far removed from the ideals of "power to the pseudo-anonymous users" of this era. Similar scenarios could

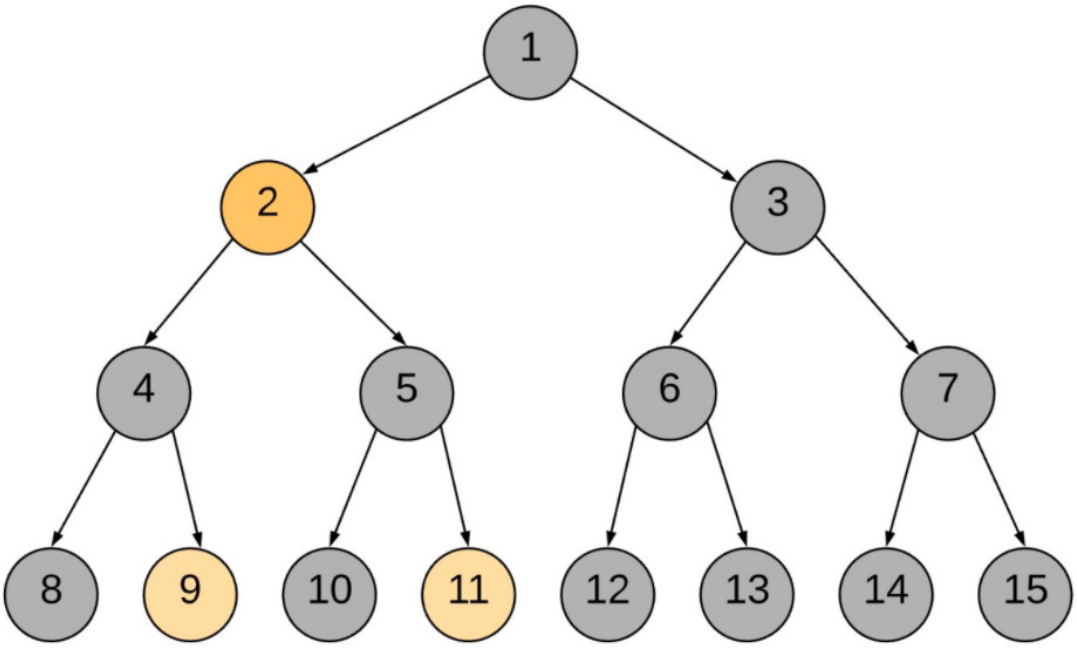
[17] 'Alternative Dispute Resolution Mechanism in India' (*IlearnCanada* 8 August 2023) <http://www.ilearncana.com/details/Alternative-Dispute-Resolution-ADR/1451> accessed 15 March 2024.
[18] See Nick Szabo, 'Trusted Third Parties are Security Holes' (*Satoshi Nakamoto Institute* 2001) <https://nakamotoinstitute.org/trusted-third-parties/> accessed 15 March 2024.
[19] ibid.
[20] Chase (n 15) 48.

be repeated in similar social contexts.

In this direction, users will be more likely to mediate problems in a fully decentralised manner, keeping total control over the process[21], rather than passively accepting a decision imposed on them from someone they do not trust and from which they run away.

To support this argument, we quote an interesting perspective from the world outside of law. Balaji Srinivasan, former CTO of Coinbase, recently made a series of tweets that perfectly embody this need for control and independence. The topic was dispute resolution tools in social networks. He defined them as a combination of anarchy (people yelling) and tyranny (arbitrary de-platforming) and proposed an alternative approach based on a global moderator hierarchy. In the event of dispute, the lowest common ancestor mediates.[22]

FIGURE 3. Global moderator hierarchy - Lowest Common Ancestor for Node 9 and Node 11 is Node 2



[21] See Giuseppe De Palo and Mery B Trevor, *EU Mediation Law and Practice* (OUP 2012). See also Penelope McRedmond, *Mediation Law* (1st ed, Bloomsbury Professional 2018).

[22] Balaji Srinivasan (@balajis), Twitter, 15 July 2021 <https://twitter.com/balajis/status/1415650556375232515> accessed 15 March 2024.

The vision of mediation as a way to escape from "tyranny" becomes clearer between the lines of the following Srinivasan's tweet:

"A seemingly paradoxical idea is that greater decentralization may allow greater centralization. If you can exit at any time, you may be more willing to delegate control on a daily basis to a centralized actor. Trust because you don't have to trust"[23]

The mediator has no binding decision-making power and therefore, even if it is a third-party, it is a decentralised one that certainly does not represent a "security hole". Through non-adjudicative processes such as mediation, users literally have the possibility to "exit at any time" by choosing if, how and when to resolve their dispute. The mediator is certainly a third-party, a third-party that acts as facilitator, that helps the disputants to work on their negotiation margins, but remains in any case a decentralised one that can never represent a risk concern for users. In Srinivasan's words, they might trust mediation because they do not have to trust.

For this reason, such an approach is more peer-to-peer and so more blockchain-friendly compared to purely adjudicative solutions. In a market of the future oriented towards "individual sovereignty" and "individual autonomy", tools such as mediation could reawaken in users a desire for independence that they already have - otherwise they would not have found themselves in the blockchain - but of which they are not yet aware.

3 Blockchain odr start-ups and security holes

The reason why the above-mentioned "cultural inquiry" has never been investigated by anyone is that in this lawless land the dispute resolution processes currently used come mainly and inevitably from the private sector. The inevitability of the on-chain privatisation of dispute resolution processes is again a logical consequence of the growing distrust against traditional courts and classic ADR methods. Many blockchainers will not be inclined to return to the centralised side after trying the decentralised one[24], which is why they try to solve their problems on-chain, by relying on a number of ODR start-ups from the private sector, known to be profit-oriented rather than culturally sensitive.

There are a number of companies that arbitrate disputes using anonymous TTPs. The following table shows some of the start-ups (e.g. Kleros, Aragon and Jur.io) currently operating in this sector.

[23] ibid.
[24] James Metzger, 'The current landscape of blockchain-based, crowdsourced arbitration' (2019) 19 Macquarie Law Journal 81, 87.

TABLE 1. Main blockchain dispute resolution projects

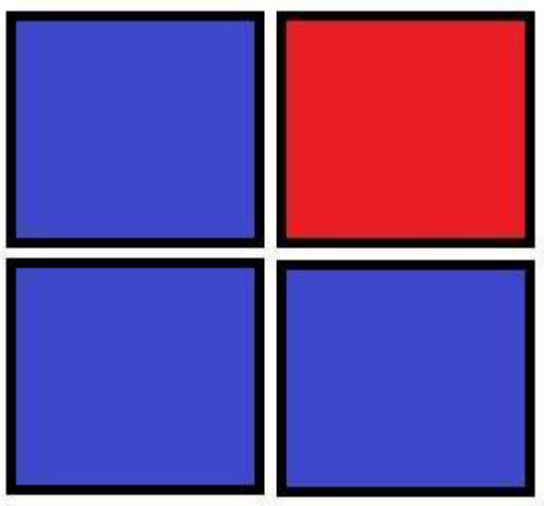
	Kleros	Aragon	Jur.io
Dispute Resolution Method	Arbitration	Arbitration	Arbitration
Modality	Plug and play (crowdsourced)	Plug and play (crowdsourced)	Embedded in Smart contract
Automatic	No	No	No
Vote method	Schelling	Schelling	Schelling
Working	Yes	Yes	Yes
Blockchain	Agnostic	Ethereum	VeChain

Existing solutions allow maintaining this concept of individual sovereignty and isolation from central control by choosing the arbiters (jurors, guardians, etc.) through a crowdsourcing process that guarantees decentralisation using a random draw of decision-makers. The latter are incentivised to act correctly with a system that assures group behaviour in tacit coordination, i.e. the Schelling point[25] (actually used by the main dispute resolution providers operating in the blockchain market).

[25] See Michael Abramowicz, 'The Very Brief History of Decentralized Blockchain Governance' (2019) 14 GW Law School Public Law and Legal Theory.

This approach guarantees decentralisation as it allows a common solution to a problem among different anonymous users (the arbiters), who do not know each other and therefore cannot communicate directly between them. An example from the world outside the blockchain is given as an illustration:

FIGURE 4. Representation of the Schelling point application out of chain.



Suppose two users have a panel in front of them with four squares, three blue and one red. They both win a prize if and only if they select the same square and they cannot talk to each other to ask the other user which square he/she is going to select. Reasonably, both will select the red square: it is not a better square than the others; it is just the square that, in a sense, stands out. The key idea taken up by Kleros, Aragon or Jur is that if a set of arbiters votes consistently, then the majority of this set will probably propose the correct solution to the dispute. In a sense, uniformity is rewarded.

In Kleros[26], the number of arbiters is 1, 3 or 5. Anyone can play this role, but in order to participate it is necessary to stake a chosen amount of Pinakion (the Kleros token). The higher the number of tokens in stake, the greater is the probability of being selected as a decision-maker. The selected arbiters propose their solution to the dispute, and at the end of the process those who voted for the most proposed decision receive an amount of Pinakion in return, while arbiters who did not vote uniformly with the others are penalised.

[26] *See* Clément Lesaege, Federico Ast and William George, *Kleros Short Paper v1.0.7* [2019] White Paper <https://kleros.io/whitepaper.pdf> accessed 12 March 2024.

Similarly, the same operational model can be found in the Jur Open Layer[27] : potential arbiters must stake the JUR token and will be drawn to resolve disputes with a certain probability proportional to the tokens invested. Specifically, "the system rewards voters who stake JUR Tokens in support of the majority position at the expense of those who stake in support of the minority position"[28].

Again, the functioning of Aragon is based on the same principle: the most voted ruling outcome wins. "For example if there are 9 guardians and 4 vote "Allow", 2 vote "Block" and 3 vote "Refuse to vote", the winning outcome of that round would be "Allow", because that outcome received the most votes out of the available options"[29].

This new form of adjudicative process is certainly a better fit than traditional methods as it delegates the central authority of the judicial system to the blockchain people. Although this approach certainly represents an interesting cop-out for proponents of the blockchain enthusiasts' cultural revolution, there are issues that have not gone unnoticed by several academics and legal professionals. Buchwald emphasises the existence of current flaws and inherent weaknesses in on-chain incentivised voting[30]. The existing literature has strongly criticised the decision-making process exercised by jurors. The first problem is the impossibility of guaranteeing reliable quality standards for decision-makers. Emmert's words in this regard are particularly representative, "Kleros is inviting anybody - regardless of professional background or legal expertise - to become a "juror" in its system and participate in decentralized dispute settlement"[31] Or again, "what is the relevance of such a vote by a random number of anonymous jurors, none of which are lawyers, let alone judges, one may ask"[32].

Decentralised justice based on Schelling's game carries a high price to pay in terms of quality of service. Even if jurors are incentivised to act in a fair manner, they remain anonymous in any case, and this prevents guaranteeing standards of competence. The delicate role of choosing what is right and what is wrong is attributed to individuals with unknown decision-making capacities. Specifically, to become a juror in Kleros no personal information is required and there is no registration process, thus making it

[27] Jur, *Open Justice Platform v3.0.0* [2021] White Paper <https://jur.io/wp-content/uploads/2021/03/jur-white-paper-v.3.0.0.pdf> accessed 12 March 2024.
[28] ibid.
[29] Aragon user guide (2021) <https://help.aragon.org/collection/1-aragon-user-guide> accessed 12 March 2024.
[30] See Michael Buchwald, 'Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration' (2020) 168 University of Pennsylvania Law Review 1369, 1423.
[31] Frank Emmert, 'A Critical Review of the Kleros "Dispute Revolution"' (*Research Gate*, 10 September 2019) https://www.researchgate.net/publication/335715800_A_Critical_Review_of_the_Kleros_Dispute_Revolution/link/5d777776299bf1cb80954c5c/download> accessed 12 March 2024.
[32] ibid.

potentially possible for anyone to become an arbiter and to be potentially dangerous with his/her decisions[33].

Again referring to Kleros, Murphy criticises the use of what he calls the 'self-professed experts'. "In a normal court, expert witnesses are expected to be able to prove why they should be acceptable to the court. This is based on educational and professional qualifications. There is no reason why this should be the case for Kleros. In fact, it could be argued that as the jurors are both bidding for work and getting paid for their arbitration, their skills should be provable and recorded"[34].

This kind of reflection also involves Aragon, whose functioning has been analysed by Kaal and Calcaterra. According to them, the adoption of an anonymous popular vote and a system of economic incentives may call required notions of effective, non-arbitrary, and fair dispute resolution mechanisms into question[35]. Jur partly avoids quality concerns as it provides a *Community layer*[36] that only allows certain professionals organised in groups called Communities to vote. Even if this represents an important step forward, it is necessary to point out that anyone - any JUR token holder - can create a community and decide on the members of the community, which does not entirely solve the problems of anonymity and the relative competence of the decision-makers.

These new forms of crowdsourced judicial systems have been exposed to criticism that goes beyond the quality standards of jurors but extends more generally to the application of Schelling's point for dispute resolution purposes. The popular opinion does not necessarily represent the correct opinion that is why this model “incorrectly shifts to incentivise a juror to vote for an outcome that diverges from the 'right' legal result”[37]. Specifically, the decision-maker is selfishly interested in not losing the stake and predicting how the co-jurors will vote rather than thinking about the well-being of the disputants. A profit-oriented approach that distances itself from the interests of the litigants represents a fallible dispute resolution process in all those disputes that are economically unattractive. “Supposedly, a lazy juror would be punished because he would be too often out of sync with the majority and lose his deposit too many times. But what if all or most jurors become lazy because the cases are just not worth any real effort? It seems at least possible that the system would become one of "first impression"

[33] See Kleros, ‘The Kleros Juror Starter Kit’ (*Blog Kleros*, 12 March 2024) <https://blog.kleros.io/the-kleros-juror-starter-kit/> accessed 12 March 2024.
[34] Ian Murphy, ‘Would You Use The Justice Protocol from Kleros?’ (*Enterprise times*, 23 January 2018) <https://www.enterprisetimes.co.uk/2018/01/23/use-justice-protocol-from-kleros/> accessed 12 March 2024.
[35] Wulf A Kaal and Craig Calcaterra, ‘Crypto Transaction Dispute Resolution’ (2017) 73(1) The Business Lawyer 109.
[36] Jur (n 27).
[37] Buchwald (n 30) 1405.

voting...”[38]. Ethicality - intended as "the ability of the system to be perceived as fair by the community"[39] - seems to be a major concern for decentralised justice.

The final flag regarding these forms of on-chain arbitration concerns the absence of discovery compulsion mechanisms. While in off-chain forms of arbitration it is possible to compel production of documents or testimony, in on-chain ones this cannot happen because of pseudonymity, which implies a lack of access to and power over the parties and their assets[40]. The Juror exercises decision-making power by assessing only two types of evidence. On the one hand, he/she will have at his disposal elements in favour of the party submitting the material; on the other hand, elements aimed at discrediting the other party. Buchwald points out that limiting the decision based solely on these two sources is not sufficient as all the evidence that inflicts self-harm is omitted. “On-chain, this third source of information falls into oblivion. Even in the simplest of disputes, the proverbial "smoking gun" disappears behind a wall of blockchain pseudonymity, presenting major opportunities for deceitful-but not impermissible-omissions”[41].

The risk of running into an incompetent juror that could be called “trusted” within the limits of their unknown skills, with the risk of suffering a decision whose logic is far from the interests of the litigants and which may not consider essential evidence due to the impossibility of having discovery compulsion mechanism, exponentially increase the possibility of inserting a decentralized security hole in the transaction.

Non-adjudicative methods gloss over this set of problems, as possible security holes can be avoided by not delegating decision-making power to third-parties, who lack legal expertise and who may make questionable decisions by carrying the heavy burden of justice. Eventually, the idea of “exit at any time” suddenly becomes more attractive.

In conclusion, while Chase's cultural inquiry has not been explored by the private sector, the result of a little reflection on it may be of interest to users interacting with these platforms. Metzger highlights the presence of economic barriers to entry: “the Kleros curated token list court currently requires that prospective jurors stake 80,000 PNK, with a value as of this writing of over $600 AUD, for the possibility of being selected as a juror. Even though the majority of that stake is likely to be returned to any juror (whether in the majority or minority of a decision), it is still a large investment in tokens that must precede participation”[42]. If we consider the countries where cryptocurrency use is most common, i.e. in Africa, Southeast Asia and Latin America[43] -

[38] Emmert (n 31).
[39] Ast and Deffains (n 13) 17. *See also* Daniel Dimov, *Crowdsourced Online Dispute Resolution* (Leiden University Center for Law and Digital Technologies 2017).
[40] Buchwald (n 30) 1400.
[41] ibid 1395.
[42] Metzger (n 24) 101.
[43] Katharina Buchholz, ‘These are the countries where cryptocurrency use is most common’ (*World Economic Forum*, 18 February 2021) <https://www.weforum.org/agenda/2021/02/how-common-is-cryptocurrency> accessed 12 March 2024.

where average monthly salaries are well below what is required to become a juror - then decentralised justice risks becoming an oligarchy of rich millennials from advanced countries. For many, this could be even more unpleasant than the central control from which blockchainers instinctively flee.

4 A new prototype for an anonymous dispute resolution process

"Aspera prototype" provides a service designed for smart contract dispute resolution through an interactive mediation process based on artificial intelligence systems. Our Mediation Clause is pluggable and potentially available for any smart contract. Both parties have the possibility to activate the clause and start the mediation process. Our prototype represents an innovative and non-adjudicative process which will be described in the next section.

The process is organised in three phases in order to ensure a sufficient level of flexibility. Specifically, it is assumed that simpler disputes will be resolved in *phase 1* or *phase 2* without the need for human support, while more complex disputes will be resolved in *phase 3* through a professional mediator and specific guarantees provided through Artificial Intelligence systems.

Suppose two parties, A and B, have a trade transaction through a smart contract. B is the buyer, while A is the owner of the contract. B starts a first transaction, sending an amount of cryptocurrency to the contract in exchange for a service provided by A. However, the buyer, after having paid, is not satisfied by the service. B can interact again with the contract, activating a specific function that starts the Aspera Mediation Clause. The clause management process can be divided in several steps:

Capital Freeze: When a user interacts the first time with the smart contract, a sum representing a fraction of the value of that transaction is automatically frozen. A and B cannot recover the frozen sum until they end the dispute or a certain period of time passes. This step is necessary because it discourages parties from running away with money and at the same time discourages them from activating the clause for futile reasons.

Chatbot Communication: After the beginning of the dispute, chatbots (ie, Artificial Intelligence) come into play. They can be used to perform a list of predetermined questions to the two parts, in order to acquire more information about the dispute. As the process progresses, more advanced chatbots will be introduced and programmed with the ability to learn over time: the more they will interact with parties, the higher the number of disputes, and so the smarter they will become. Subsequently, chatbots send the collected pieces of information to specific datasets, whose size will grow over time.

Machine Learning and Mediation reframing: Aspera uses Machine Learning (ML) algorithms to produce the mediation proposal. In this kind of approach, ML algorithms will be performed on the pieces of information previously collected on the dataset, in order to define an agreement for the parties, which is highly likely to be accepted. It is expected to get better mediation proposals as the time passes, since ML algorithms perform better when the number of data is higher. The aforementioned dataset is also used by specific algorithms in order to present a "Mediation Reframing" to each of the parties in a reciprocal manner. This is a technique of reframing the viewpoints of the disputants through changes in words or syntax, aimed at modifying the way a thought is presented so that it retains its fundamental meaning by emptying it of conflicting elements, thus achieving an optimal environment for dispute resolution.

In order to protect the confidentiality of our customers and the principles of blockchain our AI will perform on non-personal data (NDP), our chatbots will not ask personal questions. The interest is exclusively in understanding the context of the dispute and the margins for improvement on conflicting positions.

Having reached this stage, parties A and B have two options (*phase 1*). On the one hand, they can accept the mediation proposal; in this case the agreement accepted by the parties will be binding for them since the smart contract will be automatically instructed and consequently the blocked funds will be released. On the other hand, they can reject the mediation proposal and therefore disagree with ML: in this case, chatbots will interact again with the parties requesting information on the reasons that led the parties to reject the first proposed agreement, as well as additional specific questions. The information obtained from this additional round of chatbots will be transferred into the dataset. The solution proposed will then be communicated to the parties. This new proposal can again be accepted or rejected (*phase 2*). If it is accepted, the agreement reached by the parties will be binding for them as it will automatically instruct the smart contract and consequently the blocked funds will be released.

If the second agreement is also rejected, the parties will agree on a date to access the Aspera Virtual Camera for anonymous mediation (*phase 3*).

Aspera Virtual Camera for Anonymous Mediation: In this last phase, it is possible to mediate the dispute “face to face” with a human mediator but in complete anonymity in accordance with the principles of blockchain. This system allows users to meet in virtual rooms where privacy is guaranteed through artificial intelligence systems. Specifically, the AI 'masks' the physiognomy of the face and voice of those who connect, making them unrecognisable. The mediator, by accessing this room, will be able to help the anonymous parties to reach an agreement more efficiently, as he will have at his disposal the answers of the chatbots as well as the two previously rejected agreements, useful to organise a winning strategy starting from a context of the dispute that is

already well defined and clear. Through live deep fakes, it is possible to change the user's face to someone else's in real time video applications:

Figure 5. A deepfake example. Source: https://github.com/alew3/faceit_live3

This live mediation will have an exclusively facilitative purpose. Phase 3 will conform to the general principles provided by the Directive 2008/52/EC[44]. In order to ensure flexibility we intend to adopt the "Fiverr" business model. This approach will ensure an ecosystem of professionals providing mediation services at various price ranges accessible to all budgets, from a fresh graduate student with a focus on ADR who will ask for low mediation fees, to a certified mediator with multiple years of experience who will certainly ask for a larger sum. Each party will select a list of preferred mediators. One of the mediators selected by both parties will be called to mediate. Users will be able to choose a mediator according to the price they ask and the skills they have.

For users who do not embrace decentralisation and do not want to mediate disputes then it is inevitable to be exposed to the risky and intrusive judgement of a TTP. This is why there is a (phase 4) of arbitration, which we hope will be perceived by blockchainers as an *extrema ratio* for the reasons stated above. The same operational criteria will be applied here as in phase 3. Similarly to the process described for mediators, one of the arbiters selected by both parties will be called to decide. However, unlike phase 3, users will not be aware of the identity of the arbiter they have both selected until the dispute has been concluded. They will know that one of the arbiters selected in their lists will decide their dispute, but they will not know specifically which one, in order to avoid anonymous users trying to contact the decision-

[44] Directive (EC) 2008/52 concerning certain aspects of mediation in civil and commercial matters [2008] OJ L136/3 3-8.

maker separately to influence his decision. In the long term - through cryptography - it will be possible to reveal the identity of the arbiter after the dispute has been resolved, proving that it was that specific professional who decided in phase 4.

In a user-side perspective, the added values that our users would get from including the Aspera Mediation Clause in their smart contracts are as follows:

Cost savings: The combined use of chatbots and Machine Learning algorithms allows us to produce mediation proposals for phases 1 and 2 at almost zero cost, guaranteeing a dispute resolution process with a highly competitive pricing policy.

Informal approach/ Confidentiality: We do not ask our users to submit documents to prove their positions in order to establish who is right or wrong. Moreover, no witnesses or legal expertise are required. One of the main reasons why users prefer blockchain is anonymity, asking for documentation as proof does not fit their need for privacy

Faster outcome: Thanks to an automated process, once users have answered the chatbot's questions we are able to produce a mediation proposal within an hour, without having to wait for the human third-parties.

Total control over the outcome and risk management: With Aspera our users can choose whether to accept the mediation proposal or not.

Anonymity protection: We guarantee the anonymity and privacy of our users with the latest technology. In phase 3, Artificial Intelligence systems are used specifically for this purpose.

Preserve relationships: Through Aspera the dispute is resolved amicably, with an agreement accepted by both parties. This is particularly useful in the business world where it is important to maintain a good commercial relationship with clients even in case of a dispute.

Independence from third-parties with decisional power: Users are in the blockchain because they do not trust third parties and do not want to be controlled. This is why in Aspera there are no third parties deciding for them.

Possibility to feel heard: Chatbots allow users to feel heard and to express their personal views on the dispute. Users' responses are the central element for us and they are sure to be actively considered.

Multiple choice: Our users will be able to choose between three mediation agreements that will be proposed during the three phases of the process. Specifically, they will be able to choose if, when and how to resolve their dispute.

Customisation of the agreement: The use of a 3-step process permits the customisation of agreements. If the first mediation proposal is not considered "fair" by the users, they can explain why they did not accept it, and the second one will be readjusted according to the negotiation margins of the parties.

High quality standards: Phase 3 mediators will not be anonymous and will guarantee demonstrable standards of quality and professionalism.

Rating: Users will be able to assess the quality of the process and the skills of the person who handled their dispute.

Mediation Audit: We will provide an audit process based on a survey of practising mediators in the Aspera ecosystem.

Service available on a 24/7 basis: At any time of day or night, our users can activate the clause and immediately talk to the chatbot.

From a purely legal perspective, we deal with cross-border disputes using multi-language processes. As of 2021, blockchain disputes resolved by major players are related to DAOs[45], digital identity (proof-of-humanity protocol[46]), decentralised social media, freelance services, token minting and transfer.

For those unwilling to reveal their identity, the accepted agreement will be made self-enforceable on-chain. For those who are willing to step out of pseudonymity, it will be possible to make mediation agreements enforceable in countries that have ratified the Singapore Mediation Convention[47] - similarly to what is currently done in the blockchain market with arbitration awards made enforceable under the New York Convention[48] .

[45] See Alexandra Sims, 'Decentralised Autonomous Organisations: Governance, Dispute Resolution and Regulation' (DPhil thesis, University of Auckland Business School 2021).
[46] Proof of Humanity, 'The Internet for Humans' (*Proof of Humanity*, 12 March 2024) <https://www.proofofhumanity.id/> accessed 12 March 2024.
[47] United Nations Convention on International Settlement Agreements Resulting from Mediation (adopted 20 December 2018, entered into force 12 September 2020) 3369 UNTS.
[48] ibid.

5 Conclusion

Commercial disputes arising in this particular socio-cultural context cannot be resolved by readjusting the dispute resolution operating modes applicable out of the blockchain world – mostly adjudicative. New approaches are needed that strongly consider blockchainers as atypical subjects, different from the ordinary user personas. Specifically, it is necessary to design ODR systems that are a reflection of the disputes they aim to resolve, their cultural framework and the particular relational dynamics of an increasingly peer-to-peer world. The currently available adjudicative solutions may eventually turn into new forms of unexpected decentralised security holes. On the contrary, non-adjudicative methods are far from all the problems that inevitably face decentralised justice and are the perfect expression of this specific counterculture that rebels against external impositions.

This user-centred view of blockchain cannot be ignored while designing an ODR system. The need for independence and the commercial security concerns of this new era could be useful tools that legislators could exploit to promote the widespread adoption of the amicable dispute resolution methods that they have long been trying to achieve out of chain. Independence requires cooperation of the oppressed against the oppressor and mediation can be the symbol of this new independence movement. Non-adjudicative processes can bring us closer to a future where everyone manages their own transactions and cooperates in a TTP free business friendly environment. This is why it is possible to achieve total decentralisation through non-adjudicative methods, finally bringing trust in a not-trusted technology.

Elena Napolitano[*]

THE NEW FRONTIERS OF TRUST: BITCOINS AND CRYPTOCURRENCIES

Abstract

The opportunity offered by digital innovation to create new categories of goods or, at least, to transform what was previously represented by objects into something virtual has inevitably raised the issue of the legal qualification of digital assets, particularly cryptocurrencies. This classification requires a careful delimitation of the phenomenon. First, because not all 'digital representations of value' perform the same function and, most importantly, because their legal nature should be harmonised with the need to guarantee exclusive and absolute use by their owner and therefore, with tools that protect the individual's ownership rights. One fundamental effect of digital assets being qualified as property is that they can be the object of trust. Moreover, it is precisely in this context that, owing to changing economic and social demands, the need to rethink the traditional categories of civil law becomes even more acute.

JEL CLASSIFICATION: K11, K20, K24, K40

SUMMARY

1 Introduction

The digital revolution transforms, destroys and creates activities and functions in the field of trade, generating a change in human relations that inevitably affects the law, especially its function as an instrument of protection and conflict resolution.

The first problem concerns the need to understand the phenomenon and gain knowledge about matters outside the traditional sphere of jurists.

The second problem is related to the rapid and continuous pace of technical digital change that cannot be immediately summarised and translated into a suitable regulatory instrument, given the slowness of the legislative process.

[*] Honorary Fellow in Comparative Private Law, Università degli Studi della Campania 'Luigi Vanvitelli', Italy.

It is precisely in this situation that we have to contextualise the issue of the legal classification of virtual currencies. This not only requires careful delimitation of the phenomenon, since not all 'digital representations of value' perform the same function, but mainly, their legal status as to be harmonised with the need to safeguard exclusive and absolute use by their holder and therefore with tools that protect the individual's ownership rights.

It is essential, therefore, that the 'sectiorisation of law' upholds the unitary application of the legal system, where principles and values are the hermeneutic keys to the system.

It is in this perspective that it is necessary to see harmonisation as moving beyond the commercial rationale of intellectual property and extending the applications of the ownership model, involving a gradual expansion of the 'intangible assets' category to meet the demands of the virtual world and the safeguard of individuals.[1]

The inclusion of bitcoins and cryptocurrencies in the context of 'intangible assets' means an attempt to consider these 'new assets' as susceptible to appropriation and, consequently, the object of ownership. It is, therefore, necessary to address a broader phenomenon which, as is well known, has, for some time, been the object of fascination in both civil law and common law contexts. Thus, taking advantage of these different approaches in legal comparison will provide a better framing of the different legal systems, while highlighting issues of global significance.

The many applications developed include the use of trusts as a vehicle for collecting virtual monetary assets. This is because the physiological fear that accompanies any recourse to legal schemes that do not belong to the civil law tradition has now been overcome.

Moreover, it is precisely in this context that, owing to changing economic and social demands, the need to rethink the traditional categories of civil law becomes even more acute.

As authoritative doctrine has argued, 'property, from two different perspectives, is a subjective situation and a relationship'. [2]

In structural terms, ownership is expressed as a relationship between the owner's circumstances and the potential competing circumstances of third parties.

However, the owner's circumstances presuppose an obligation of conduct on his or her part, a duty to abstain and an obligation to cooperate with the other owners with the potentially opposing interests.

---

[1] Pietro Perlingieri and Pasquale Femia, *Nozioni introduttive e principi fondamentali del diritto civile* (Esi 2004) 125. *Status personae* and *status civitatis* are «*situazioni precise con contenuto tipico o atipico determinato. Sì che per tali qualificazioni è possibile individuare quali servizi e beni sono essenziali*». See Pietro Perlingieri, *Il diritto civile nella legalità costituzionale IV Attività e responsabilità* (ESI 2020) 261.

[2] Pietro Perlingieri, 'Relazione conclusiva' in Ernesto Capobianco, Giovanni Perlingieri and Marcello D'Ambrosio (eds), *Circolazione e teoria dei beni* (ESI 2020).

Thus, the functional aspect is prevalent in ownership as a relationship[3] between the owner and the third party, be it a private individual or a public body. Cooperation is required, where sometimes the interests of the owner are prevalent and sometimes those of the third parties. What is certain is that defining the social function of ownership as a criterion of sound economic management seems reductive, given the changed fundamental values in the legal system.

'Considering the centrality of the value of the person in the constitutional system with the consequent functionalisation of the patrimonial situations – property and business – to existential situations',[4] the need arose, therefore, to protect all projections of the individual into the virtual world that are accessed via a digital identity,[5] defined as the virtual representation of a person's identity used as a means of connection between the real world and the digital world.[6]

Thus, jurists cannot overlook this social phenomenon, since the law is itself a social phenomenon,[7] changing over time as 'the product and at the same time the engine of cultural, economic, social and political changes'.

'This is more necessary because scientific and technological innovation is the bearer of an incessant change that cannot be governed through the traditional pursuit of legislation. It is indispensable, therefore, to prefer "forward-looking" instruments, such as those linked to a norm based on principles'.[8] At the same time, constructing a discipline based on closed cases presupposes a law that intervenes at the end of a cycle, to select and reorganise interests and situations that are now consolidated. However, the law may choose – given the specific sector in which it is to be applied – the path of *sunset provision*, rules that will disappear and be replaced at a predetermined deadline, thereby creating an obligation on the legislator (or others) to reconsider the matter.[9]

2 Digital innovation and the theory of goods

In the last decade, the legal debate on the circulation of trust[10] has aroused particular interest among European jurists. This attention is due to the opportunity granted by digital innovation to create new categories of goods or, at least, to transform

[3] ibid 102.
[4] Perlingieri (n 1) 295.
[5] Vincenzo G Giglio, '*Identità e profilazione digitale: i rischi dei Big Data*' (*Filodiritto*, 22 November 2016) <https://www.filodiritto.com/identita-e-profilazione-digitale-i-rischi-dei-big-data> accessed 25 March 2024.
[6] Massimo Giuliano, 'La blockchain e gli Smart Contracts nell'innovazione del diritto del terzo millennio' (2018) 6 Il diritto dell'informazione e dell'informatica 989.
[7] Salvatore Satta, *Colloqui e soliloqui di un giurista* (CEDAM 1967) XIX.
[8] Stefano Rodotà, *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione* (Laterza 2004) 23.
[9] ibid.
[10] In this regard, see Raffaele Lener, 'La circolazione del modello del trust nel diritto continentale del mercato mobiliare' (1989) Rivista delle Scoietà 1050 ; Antonio Gambaro, 'Il trust in Italia e in Francia', in Paolo Cendon (ed), *Studi in onore di Rodolfo Sacco* (Giuffrè 1994) 495 .

what was previously represented by objects into something that is virtual. Thus, a transposition of reality, though not through material elements but rather through numbers and therefore algorithms capable of translating reality into electronic information and algorithms in turn capable of transforming this information into something for the end user.

Technology has always had a significant influence on how associates regulate their relationships, thus, indirectly, on the laws that governs society.[11] This opens up vistas for legal research in the field of property law (Book III, Title I of the Italian Civil Code) and the relationship between these and rights in rem (Book III of the Italian Civil Code). The issue has been addressed more as it relates to intellectual property and intellectual and artistic works as opposed to property per se, and focuses on what digital innovation has brought to the existing categories, as a result of the flexibility of Italian law; but also how this limits the need to develop a broad, comprehensive theory of digital goods and contracts.

The notion of 'rights over intangible assets'[12], now formally in disuse, has given way to 'intellectual property', which is characterised as a summary formula for a vast array of legal situations concerning incorporated things. The so-called 'protectionist drift of intellectual property' was then followed by a significant process of 'constitutionalisation' of the legal situations in question. Over time, intellectual property has been elevated to a constitutionally protected right.

The crucial stages in this process are clearly observed in the Court of Strasbourg's recognition of intellectual property as a protected possession under the First Protocol of the ECHR, and also in its formal inclusion in the general guarantee of ownership provided for by Article 17 of the EU Charter.[13]

The confluence of technological evolution, changes in economic structures and the evolution of the institutional framework has led to various consequences that increasingly underscore the self-referential paradigm of intellectual property.[14]

The change in the lexical order reflects a profound evolution at the regulatory level,[15] where the theory of goods is not limited to the theory of rights in rem or to that of property[16]. Emblematic of this is the study of information as a commodity.

[11] Giovanni Pascuzzi, *Il diritto dell'era digitale* (Il Mulino 2002) 61, 66.
[12] Gustavo Ghidini, 'Prospettive "protezionistiche" del diritto industriale' (1995) I Rivista di diritto industriale 73.
[13] Marco Ricolfi, 'Sub art. 17, c.2', in Roberto Mastroianni, Oreste Pollicino and Silvia Allegrezza, *Carta dei diritti fondamentali dell'Unione Europea* (Giuffrè 2017) 338; Laurence Helfer, 'The New Innovation Frontier? Intellectual Property and the European Court of Human Rights' (2008) 49 Harvard International Law Journal 1.
[14] Alexander Peukert, 'Guterzuordnung und Freiheitsschutz', in Reto M Hilty (ed), *Geistiges Eigentum: Herausforderung Durchsetzung* (Springer 2008) 47.
[15] Giorgio Resta, 'Dal dominio delle cose all'esclusiva sui beni immateriali' in Capobianco, Perlingieri and D'Ambrosio (n 2) 27.
[16] The so-called objectivist conception solves the problem of property in the theory of goods: Pietro Perlingieri, *Introduzione alla problematica della proprietà* (ESI 2011) 85.

Legal theory has asked whether information is a legal asset, whether and when it can form part of a legal relationship and by what means it can be protected. It has been argued that the solution requires that the information has an appreciable social utility and, at the same time, finds its unity in the legal system, an evaluation of merit.[17]

In principle, it is essential to establish a realistic and correct relationship between the content – document or medium – and its content (the news or idea), without insisting on protecting one another. All this is necessary, considering that the distinction between content and its support in today's digital reality is somewhat nuanced. However, they are suitable as references of interests and subjective legal situations.[18] In a socio-historical context characterised by the increasing importance of interests and utilities[19] which, on one hand are devoid of materiality and, on the other, have none of the exclusivity that is typical of real situations, a different orientation would reveal all its inadequacy.[20]

One example, possible today thanks to digitisation and blockchain, is so-called 'tokenisation' [21], namely the reduction to a numerical code of any right to be used on an asset in order to make it exchangeable. One would have to ask the meaning of attributes of goods such as 'fungibility' and 'consumability', but also which contracts concern such goods and whether it still makes sense to talk, say, contracts for the escrow and administration of dematerialised financial instruments no longer represented even by an accounting entry (object of the case), but by a unique numerical code that identifies the single instrument, the single right, its holder and the previous holders. There is,

[17] Pietro Pelingieri, 'L'informazione come bene giuridico' (1990) 2 Rassegna di Diritto Civile 338.
[18] Pietro Perlingieri, *Il diritto civile nella legalità costituzionale. Vol III* (ESI 2020) 323, 324.
[19] Cf. on the topic, Giorgio de Nova, 'I nuovi beni come categoria giuridica' in Giorgio de Nova, Bruno Inzitari, Giulio Tremonti and Gustavo Visentini (eds), *Dalle res alle new properties* (Jovene 1991) 13; Antonio Gambaro, 'La proprietà nel common Law anglo-americano', in Albina Canadian, Antonio Gambaro and Barbara Pozzo (eds) *Property, Propriété, Eigentum* (CEDAM 1992) 167; Bruno Inzitari 'Le New Properties nella società post-industriale', in Giorgio De Nova, *Dalle res alle new properties* (Jovene 1991) 53 ; Antonio Jannarelli, 'Beni. Profili generali', in Nicolò Lipari (ed) *Diritto privato europeo vol I* (CEDAM 1997) 380; Antonio Jannarelli, 'La disciplina dei beni tra proprietà e impresa nel codice del 1942' [1993] Rivista critica del diritto privato 46, 52; Michele Lobuono, 'I «nuovi beni» del mercato finanziario' (2002) Rivista di diritto privato 48; Ugo Mattei, 'Qualche riflessione su struttura proprietaria e mercato' (1997) Rivista critica di diritto privato 25; Alberto Pretto, 'Strumenti finanziari: la nuova proprietà' (1997) Rivista critica di diritto privato 669; Stefano Rodotà, *Il terribile diritto. Studi sulla proprietà privata* (Il Mulino, 1990) 20; Paola D'addino Serravalle, *I nuovi beni e il processo di oggettivazione giuridica. Profili sistematici* (ESI 1999); Alessandra Bellelli and Alberto Giulio Cianci, *Beni e situazioni giuridiche di appartenenza: tra diritti reali e new properties* (Giappichelli 2007); Alberto Maria Gambino, 'Diritto d'autore e nuovi processi di patrimonializzazione' (2011) Diritto industriale 114; Claudia Morgana Cascione, 'Garanzie e "nuovi beni". Sulla collateralization di nomi di dominio, pagine web, banche dati' (2010) 3 Rivista di diritto privato 69; Ilaria Garaci, *Nuovi beni e tutela della persona. Lo sfruttamento commerciale della notorietà* (Giappichelli 2012); Andrea Zoppini, 'Le «nuove proprietà» nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)' (2000) 46(2) Rivista di diritto civile 185.
[20] See Anna Carla Nazzaro, 'Nuovi beni tra funzione e dogma' [2013] Contratto e impresa 1014; Enrico Caterini, 'Il contributo del libro terzo del codice civile alla formazione del "diritto patrimoniale comune". La palingenesi della proprietà' (2011) I in Rassegna di diritto civile 1.
[21] CONSOB 'Le offerte iniziali e gli scambi di cripto-attività' (Discussion Paper, 19 March 2019) <https://www.consob.it/documents/1912911/1972122/doc_disc_20190319.pdf/2044537e-487c-5093-112e-3eacc69b12d4> accessed 25 March 2024.

therefore, a necessary connection between goods, things, and rights over things, between property and the regime of ownership, where the concept of property postulates its ability to be 'the object of rights' (Art. 810 of the Italian Civil Code), that is to say, the object of an active subjective situation, and not only of exclusive rights, in terms of ownership.[22]

In essence, only after a careful analysis of the law of assets, will it be possible to analyse the types of contracts applicable for the transmission and storage and management of such newly designed assets so they become invulnerable to adverse financial events involving the owner, thus protecting their value in the interests of the owner and their family. As will be seen below, the trust is an institution that, although not belonging to the civil law tradition, is the one that proves to be effective in pursuing these legitimate objectives.[23]

Therefore, there is a clear shift towards an economy based on a technological society that finds expression in digital information. This evolution has led to new and significant problems, primarily around the issue of qualifying cryptocurrency as a legal asset.

The traditional study of goods has proved to be wholly inadequate. It can no longer be traced back to a unitary model, but rather is fragmented due to the multiplicity of legal phenomena related to 'new goods', each with different characteristics and difficult to categorise.

The need to establish rules that can regulate actions arising and developing within a meta-territory[24] and which in turn affect the object of the law, leading to an expansion of the category of goods,[25] in order to catalogue these new phenomena and deduce their legal effects, demands adaptation on the part of the interpreter,[26] whose task is made even more difficult by the extreme vagueness of the wording contained in article 810 of the Italian Civil Code.[27]

The term 'thing', [28] to which the wording of the article in question expressly refers, includes both the portions of material reality, which fall under the dominion of the senses and are susceptible to autonomous appropriation, and the immaterial, '*res quae tangi non possunt*', which, although devoid of material consistency, are capable of

[22] Salvatore Pugliatti, 'Beni, (Teoria gen.)', in *Enc dir* V (Milan 1959) 164; Pietro Perlingieri and Pasquale Femia, *Nozioni introduttive e principi fondamentali del diritto civile* (ESI 2004) 132.
[23] Maurizio Lupoi, *Istituzioni del diritto dei trust negli ordinamenti di origine e in Italia* (4th ed, CEDAM 2019); Lucia Di Costanzo, *Il* trust *nel diritto italiano* (ESI 2022).
[24] Understood as something external, even if located in a territory recognised by the international community. On this, see Manlio Cammarata, 'Quali leggi per il ''territorio Internet''?' (1997) <http://www.interlex.it/regole/mcmeta1.htm> accessed 25 March 2024.
[25] Antonio Gambaro, 'Il diritto di proprietà', in Antonio Cicu and Francesco Messineo (eds), *Trattato di diritto civile e commerciale* (Giuffrè 1995) 129; Giorgio De Nova, 'I nuovi beni come categorie giuridiche', in De Nova, Inzitari, Tremonti and Visentini (n 19) 15.
[26] Massimo Giuliano, 'Criptovaluta e trust' (2021) 4 Trusts e attività fiduciarie 384.
[27] Massimo Giuliano, 'Le risorse digitali nel paradigma dell'art. 810 cod. civ. ai tempi della blockchain' (2021) 5 NGCC 1215.
[28] 'Cosa' *Enciclopedia Treccani online* <https://www.treccani.it/vocabolario/cosa/?search=còsa>.

providing utility, appropriation and forming an object of law, thus showing itself to be meagre, ambiguous and capable of regulating a constantly evolving phenomenon.[29]

Several scholars have pointed out that this provision contributes little to the quest for the legal concept of property, precisely because of its linguistic formulation, to the extent that it is subject to the most disparate interpretations.[30]

Traditional theory held that the concept of legal good, meaning 'any material entity or ideal of legal relevance', could be inferred from that definition.[31]

Other theories have held that it would be devoid of prescriptive value, since it does not have the function of a general normative criterion for qualifying goods in the legal sense, but would be the instrument by which 'goods' could be qualified according to the legal system and, therefore, be the object of rights.[32]

The terms 'good' and 'thing' contained in the provision in question have received multiple and often opposing interpretations from the most authoritative exponents[33] of theory, as a result of the broad spectrum of semantic meanings attributed to them by legislators, by jurisprudence and by theory itself.

The prevailing legal theory distinguishes these concepts by considering them not to be about genus or species.[34] However, the two notions need to be clarified and used synonymously in practical application. On the other hand, a minority of and less recent theorists consider them to be interchangeable terms, assessments of the same legal entity.[35]

However, the concept of 'thing' is independent of juridical evaluations, since it is summed up in a pre-juridical entity,[36] which is identified with a portion of material reality.[37] There is no shortage of those who point out that this material physicality must be susceptible to autonomous exploitation, in both structural and functional terms.[38]

[29] Scholars have often criticised the wording of the rule. See: Vincenzo Zeno-Zencovich, 'Cosa' in Associazione italiana di Diritto Comparato, *Digesto delle discipline privatistiche. Sezione civile*. Vol IV (UTET 1989) 438. The Author observes that *'La cosa è un'entità pre-giuridica, ossia un elemento della realtà preso in considerazione dal diritto, privo di una sua autonoma qualificazione giuridica'*.

[30] Mario Barcellona, 'Attribuzione normativa e mercato nella teoria dei beni giuridici' [1987] Quadrimestre 615; otherwise, for its preceptive value, A Pino, 'Contributo alla teoria giuridica dei beni' (1948) 1 Rivista trimestrale di diritto e procedura civile 835.

[31] Bruno Biondi, 'I beni', in *Tratt. Vassalli* (IV, UTET 1953) 15.

[32] Oberdan Tommaso Scozzafava, 'Dei beni' in Piero Schlesinger, *Il codice civile. Commentario* (Giuffrè 1999) 5; Antonio Jannarelli, 'La disciplina dei beni tra proprietà e impresa nel codice del 1942', in *Letture di diritto privato* (CEDAM 1994) 97.

[33] Nicolò Lipari, *Le categorie del diritto civile* (Giuffrè 2013).

[34] '*Il granello di sabbia e la lontana galassia pur certamente esistenti nel mondo della realtà e pur costituendo cose non possono essere qualificati come beni*', in this sense Zeno-Zencovich (n 29) 439.

[35] Bruno Biondi, 'I beni' in F Vassalli, *I beni* (UTET, Torino 1953) 15, for whom a juridical asset '*qualsiasi entità materiale o ideale giuridicamente rilevante*', but *contra* Ugo Natoli, *La proprietà* (Giuffrè 1976) 70.

[36] Zeno-Zencovich (n 29) 443.

[37] Francesco Santoro Passarelli, *Dottrine generali di diritto civile* (Jovene 1976) 55.

[38] Fulvio Maroi, 'Cosa', in *Novissimo Digesto Italiano* (UTET 1938) 356; Rosamaria Ferorelli, *Le reti dei beni nel sistema dei diritti. Teoria e prassi delle nuove risorse immateriali* (Cacucci 2006) 80.

The traditional thesis, on the other hand, usually qualifies goods as material things that can be a source of utility,[39] in that they can satisfy human needs and, as such, are subject to exclusive appropriation, attributable to the right of property or other forms of possession.[40]

The *punctum dolens* is precisely this: to come to support a notion of a 'thing' that is not necessarily corporal, endorsing the thesis that maintains that the qualification of the thing as a juridical good would not rest on the logic of ownership.[41]

Other authors believe that the provision of art. 810 of the Civil Code is highly abstract and that the process of objectification of things is based on the exchange value of the things themselves, i.e. on the principle of patrimonialism, based on the assumption that, in a market economy, only the market decides what does or does not have value.[42]

Interpretation difficulties involved in outlining the complaints about the vagueness and abstractness of the provision in question, as well as the variety of meanings that are attributed to the way 'terms such as "goods" [43] and "thing" [44] are used by the legislature, by doctrine and by the case-law in the name of the widest polysemic nonchalance'[45] have not prevented legal scholars from recognising the historical and systematic significance of art. 810 of the Italian Civil Code.[46]

It is precisely the absence of a general theory of goods that is unanimously shared and suitable for considering the emergence of new forms of wealth in a globalised society that makes it difficult for the interpreter to prepare the legal instruments necessary to ensure the best functioning of technological innovations, based, fundamentally, on the knowledge and use of data,[47] also, and above all, in terms of generational transition.

Therefore it is time to move away from the conception of the 'thing' strictly dependent on the requirements of 'corporality', 'utility' and 'patrimoniality', since

[39] Rosamaria Ferorelli, 'Della proprietà, Artt. 810 – 868', in Enrico Gabrielli (ed), *Commentario del Codice Civile* (CEDAM 2012) 6.

[40] Oberdan Tommaso Scozzafava, *I beni e le forme giuridiche di appartenenza* (Giuffrè 1982) 90.

[41] Michele Costantino, 'La proprietà in generale', in Pietro Rescigno, *Trattato di Diritto Privato. Voll. VII-VIII* (UTET 1982) 18; Davide Messinetti, 'Oggetto dei diritti', in *Enciclopedia del Diritto* (XXIX, Milan 1979) 812.

[42] Pietro Barcellona, *Diritto privato e società moderna* (Jovene 1996) 229; Pietro Barcellona, *Diritto privato e società moderna* (Jovene1996) 634.

[43] Salvatore Pugliatti, *Scritti giuridici* (Giuffrè 2011) 433.

[44] Stefania Romeo, *L'appartenenza e l'alienazione in diritto romano. Tra giurisprudenza e prassi* (Giuffrè 2010) 99; Giovanni Pugliese, 'Dalle «res incorporales» del diritto romano ai beni immateriali di alcuni sistemi giuridici odierni' [1982] Rivista trimestrale di diritto e procedura civile 1137; Giovanni Turelli, ''Res incorporales' e 'beni immateriali': categorie affini, ma non congruenti' [2012] Teoria e Storia del Diritto Privato 1.

[45] Paolo Grossi, 'I beni: itinerari tra ''moderno'' e ''post-moderno''' (2012) 66(4) Rivista trimestrale di diritto e procedura civile 1059; Marco Allara, *Dei beni* (Giuffrè 1984) 8.

[46] Antonio Jannarelli, 'La disciplina dei beni' [1993] Rivista critica di diritto privato 97.

[47] On the impact of big data and algorithms on rights, see Vincenzo Zeno-Zencovich, 'Big data e epistemologia giuridica', in Alix Lloredo Alix and Alessandro Somma (eds), *Scritti in onore di Mario G. Losano* (Accademia University Press 2021). *Ex multis*, Antonio Gambaro, 'Il diritto di proprietà', in Antonio Cicu and Francesco Messineo, *Il diritto di Proprietà (*Giuffrè 1995) 129; Giorgio De Nova, 'I nuovi beni come categorie giuridiche', in De Nova, Inzitari, Tremonti and Visentini (n 19) 15.

there are emblematic examples of things included among the intangible goods, things with natural energies, where materiality is recognised despite the absence of tangibility.[48]

On the other hand, legal practitioners have often found it challenging to identify adequate regulation within the legal system in the face of the emergence of 'new assets',[49] mainly because of the difficulty of bringing these entities back within the framework of property rights. Suffice it to say that even the institution of trusts in our legal system has suffered from incompatibility with the known proprietary scheme. However, at the same time, it has made a different conception of possession (re)emerge without violating the regulatory apparatus.

Ignoring the epochal change that our society is going through under the pervasive pressure of technological progress, as the Internet has been and as *blockchain*[50] is now, where we discuss digital capitalism, '*platform capitalism*', '*platform society*' or '*immaterial capitalism*',[51] where technology companies inevitably exercise a power of control over the movement of goods, commodities and services, all rendered intangible digital entities, means denying the existence of the object of the law in most legal relationships in the information society and information technology. Thus it also means denying the possibility of exercising rights and denying protection to those who derive economic benefit from these 'objects', social and moral, and contribute to the full development of the personality, as sanctioned by art. 2 of the Italian Constitution.

What is essential, therefore, is not limited to the material consistency of the entity or the way it is apprehended, but the interest of the person to be protected, which must be legally relevant and worthy of protection.[52]

Conversely, a discipline rigidly entrusted to technical regulations would not only be inadmissible from a legal point of view, but also functionally inadequate because the

[48] Scozzafava (n 40) 1; De Nova, Inzitari, Tremonti and Visentini (n 19); Arianna Pretto, 'Strumenti finanziari, la nuova proprietà' [2000] Rivista critica di diritto privato 669; Oriana Clarizia, 'Il diritto di proprietà dal codice civile alle nuove forme di appartenenza' in Stefano Pagliantini, Enrico Quadri and Domenico Sinesio (eds), *Studi Comparati* (Giuffrè 2008) 787; Ugo Mattei, 'Proprietà (nuove forme di)', in *Enciclopedia del diritto* (Annali V, Milan 2012) 1118; Anna Carla Nazzaro, 'Nuovi beni tra funzione e dogma' [2013] Contratto e impresa 1014.

[49] Pasquale Femia, 'Il campione biologico come oggetto di diritti. Bene giuridico e processi di valorizzazione', in Dario Farace (ed), *Lo statuto etico-giuridico dei campioni biologici umani* (NEU 2016) 200.

[50] Blockchain is a digital ledger structured as a chain of blocks containing data and whose consensus on the state of the ledger is distributed across all nodes (computers) in the network. Once written to a transaction contained in a block, the data cannot be retroactively altered without modifying all subsequent blocks. Owing to the nature of the mathematical protocol and the validation scheme, this would require the consent of most of the network. However, the more distributed the network of nodes is, the harder this is to obtain. Thus, as will be said later, the data become unique.

[51] See Francesco Giacomo Viterbo, 'Freedom of contract and the commercial value of personal data' [2016] Contratto e impresa Europa 953.

[52] Scozzafava (n 40) 90, where '*un'entità diviene oggetto di disciplina giuridica quando sulla stessa si appuntano interessi umani di qualsiasi natura, che in un determinato contesto storico-culturale vengono giudicati meritevoli di tutela*'.

incessant evolution of digital techniques would also lead to the obsolescence of the legislation.[53] It follows that the spread 'intangible' and immaterial interests requires a reassessment of the traditional techniques employed to qualify subjective situations. The advent of the digital revolution thus places the interpreter before situations that are difficult to define and even more uncertain to regulate, producing a potent blend of reality and obligation.[54]

3 Historical developments leading to Bitcoin

The new communication systems and the interconnection that the network has inevitably produced have changed conceptual frameworks and ways of life, thus creating new social systems that are constantly evolving and revolutionising.

On the other hand, this has led to a more sensitive perception of the problems arising from the a-territoriality of the Internet and the presence of an interconnected system.

The web itself has undergone an apparent transformation over time: initially conceived to link various static hypertext documents together, it has evolved, beginning with the definition of Web 1.0 and the paradigm of the static web.

Using new programming languages, the relationship between the user and the web has inevitably changed, moving from a passive to an active stance, changing the philosophical approach and reaching the user who is also a content provider (Web 2.0, made up of wikis, social networks, blogs). Further trends have followed with an apparent propensity for simultaneous integration, concentration and decentralisation.[55] In this context, interactive 'virtual worlds' have appeared, up to MMOGs (Massive Multiplayer Online Games), games played on the network and simultaneously by several people. Some famous ones are *War of Warcraft*[56] and *Second Life*.[57]

The difficulties have increased with the appearance in these virtual worlds of the first virtual currencies[58] (Linder Dollar in *Second Life*), with the surprising formation of a real

[53] Pietro Perlingieri, 'Privacy digitale e protezione dei dati personali tra persona e mercato' (2018) 2 Foro napoletano.
[54] Maria Cristina Zarro, 'Il regime di tutela del dato informativo quale asset intangibile', in Capobianco, Perlingieri and D'Ambrosio (n 2) 283.
[55] Stefano Capaccioli, *Sviluppo storico sui fondamentali documenti per arrivare al bitcoin, Criptoattività, criptovalute e bitcoin* (Giuffrè 2021) 39.
[56] World of Warcraft is a three-dimensional fantasy MMORPG () fantasy video game, which can be played online for a fee.
[57] *Second Life* is an online digital electronic virtual world launched on 23 June 2003 by the American company *Linden Lab*, from an idea of the company's founder, physicist *Philip Rosedale*. It is a new media IT platform that combines synchronous and asynchronous communication tools. It is applied in multiple creative fields, including entertainment, art, training, music, cinema, role-playing games, architecture, programming, business, to name a few (source: Wikipedia).
[58] Hiroshi Yamaguchi, 'An Analysis of Virtual Currencies in Online Games' (*SSRN*, 1 September 2004) <https://ssrn.com/abstract=544422> accessed 24 March 2024; Vili Lehdonvirta, 'Real-Money Trade of Virtual Assets: New Strategies for Virtual World Operators' in Mary Ipe (ed), *Virtual worlds* (Icfai University Press, Hyderabad, India, 2008) 113, 137; Levent V Orman, 'Virtual Money in Electronic Markets and Communities' ICAST Journal of Institute for Communication, Social Informatics, and Technology, Forthcoming, Johnson School Research Paper Series No. 27-2010

economy in the virtual world and the creation of markets[59] and websites for the exchange of these currencies and the creation of a meta-currency[60] (*Open Metaverse Currency*) used to buy or sell virtual goods or services in virtual contexts, accepted in several virtual worlds.

Many of the ideas were developed by the *cypherpunk*[61] and crypto-anarchist movements, which, intent on countering the possible restrictions on freedoms and the right to privacy that the increasingly pervasive spread of information technologies would allow governments and large corporations, had identified anonymous electronic money and other untraceable payment instruments as the panacea for these asymmetries, all using large-scale cryptographic technologies.

It is practical, at the outset, to say why the unprecedented perspectives of information technology, marked not only by delocalisation, but also by the dematerialisation of activities and things within virtual spaces, and more specifically, the advent of *blockchain* technology, defined as '*disruptive*'[62], represents an extraordinary innovation in recent years.[63]

Usually, when reconstructing the phenomenon of *blockchain*, reference is made to the *paper* that appeared on a *mailing list* by a 'phantom' Satoshi Nakamoto,[64] dating back to 31 October 2008, which highlighted how a traditional economic thought can be set out using digital techniques (cryptography, transmission protocols, time stamping), giving rise to a new concept of "crypto economy".

In just nine pages, this publication laid the foundations and theorised the first *trustless* payment system based on *blockchain* technology, combining a series of already known technologies but finding innovative solutions to some problems that arise from

<https://ssrn.com/abstract=1621725>; Matthew Elias, 'Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy' (3 October 2011) <https://ssrn.com/abstract=1937769> accessed 25 March 2024.

[59] Kerry L Macintosh, 'How to Encourage Global Electronic Commerce: The Case for Private Currencies on the internet' (1998) 11 Harward Journal of Law and Technology 733, 796.

[60] One of the first sites to carry out this activity was www.virwox.com. *Massive Multiplayer Online Role-Playng Game*.

[61] From Wikipedia, 'A *cypherpunk is a* libertarian activist who advocates the intensive use of computer cryptography as part of a path of social and political change, for example by violating confidential archives to make public some inconvenient truths. Originally, *cypherpunks* communicated through a *mailing list*, in informal groups with the intent of obtaining the *privacy* and cybersecurity of personal *accounts*, through the use of encryption, against governments and economic groups. *Cypherpunks* have been organized into an active movement since the late 1980s, with influences from *punk* culture. An example of *cypherpunk activism is Julian Assange*'s Wikileaks website' <https://it.wikipedia.org/wiki/Cypherpunk> accessed 24 March 2024.

[62] So defined because it brings 'to a market a very different value proposition than had been available previously' see Joseph L Bower e Clayton M Christensen, 'Disruptive Technologies: Catching the Wave' (1995) I Harvard Business Review 10.

[63] On the methodological and conceptual limits of the more conventional approach of comparison by 'legal systems', linked to the idea of the 'territoriality' of (positive) law, shifting towards a different holistic approach, based on the idea of 'spatiality' of law as an experience that is both local/relative and global/universal, particularly in terms of globalisation and supranational legal integration (European law), see also Luigi Moccia, 'Comparazione giuridica, diritto e giurista europeo: un punto di vista globale' [2011] Rivista trimestrale di dritto e procedura civile 767.

[64] A pseudonym used by a person or group of people. See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) <www.bitcoin.org>.

the creation of a distributed payment mechanism between distant people, with the elimination of a central body to ensure the certainty of the payments themselves.

The idea of a decentralised virtual currency was first described by Wei Dai in 1998, on a mailing list of crypto-anarchists, in his proposal B-money, with which he first described a payment system guaranteed by encryption and so-called encryption *proof of stake*, i.e. the incentive of participants to act honestly in the network and otherwise lose the deposited funds in the event of validation of fraudulent transactions.

In the same years, the blogger and cryptographer Nick Szabo proposed the definition of *smart contracts*, *smart contracts* capable of automatically executing transactions. The same law student published a post in December 2005 on the concept of bit-gold, based on the idea developed the year before by Hal Finney, namely the theory of *proof of work*, but without putting a limit on the total amount of bit-gold produced and giving them a different value depending on the computational capabilities invested to produce them.

Blockchain[65] is a set of technologies that allow the maintenance of a *distributed ledger* of data, structured in the form of a continuously growing 'chain of blocks', each containing a certain number of transactions that vary depending on the type of blockchain. These blocks are linked to each other according to a chronological principle, and their integrity and immutability are guaranteed through a system of consensus algorithms and cryptographic rules.[66]

It works like a public ledger in which transactions between two users of the same network are stored. The data relating to the exchanges are saved within cryptographic blocks, hierarchically connected, thus creating an infinite chain of data blocks that allows all transactions to be traced and verified. The chain's single block contains two peculiar data: a *hash* referring to the previous block and a *timestamp*.[67]

4 The legal qualification of virtual currencies

For some time now, *blockchain* has established itself as a new technology for managing electronic transactions, allowing the validation and archiving of reports, and ensuring their traceability, security, and execution in terms of payment.

[65] The term 'blockchain¢ is a combination of the words '*block*' and *'chain'*. On this subject, see Michéle Finck, *Blockchain regulation and governance in Europe* (CUP 2019); Raffaele Bianchi, Gianluca Chiap and Jacopo Ranalli, *Blockchain: tecnologia e applicazioni per il business* (Hoeply 2019); Primavera De Filippi and Aaron Wright, *Blockchain and the law*, (Harvard University Press, 2018); Nicola Attico, *Blockchain, guida all'ecosistema: tecnologia, business, società (*Guerini Next 2018); Copier Berbain, 'La blockchain: concept, technologies, acteurs et usages' (2020) 2 Annales di Diritto e pratica tributaria internazionale 2.
[66] The set of ciphers that enables verification of users' identities is called a cryptographic key.
[67] Antonio Tommasini, *Criptovalute, NFT e Metaverso* (Giuffrè 2022).

On this point, the *European Banking Authority*[68] has identified *virtual currencies* based on an economic-functional approach. From the subdivision made, we can talk about virtual payment currencies, which represent payment instruments (Bitcoin, Ethereum)[69]; virtual investment currencies, used both as a claim against the issuer and as a right to a shareholding[70]; virtual currencies of use, which allow you to access and use a digital service.[71]

From this, it is necessary to consider the phenomenon of cryptocurrencies,[72] which, in the only (generic) definition available offered by anti-money laundering legislation, constitute *digital representations of value* or rights used as 'medium of exchange or held for investment purposes'.[73]

Next, that directive defines *virtual currencies* as 'a representation of digital value that is not issued or guaranteed by a central bank or public body, is not necessarily linked to a legally established currency, does not have the legal status of monetary

[68] See EBA, *Report with advice for the European Commission* (9 January 2019) 7. However, at the national level in Switzerland, for an initial overview by type and function of cryptocurrencies, see FINMA, 'Practical Guide for the Processing of Applications for Initial Coin Offerings (ICOs)' (16 February 2018) <https://www.finma.ch/it/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=it&hash=8C6FAD033EDB1A4963AC6E2BE2E013BE>. In doctrine, v. Christofer Hahn and Adrian Wons, *Initial Coin Offering (ICO)* (Wiesbaden 2018*)* 15.

[69] Daniele Minussi, 'Utilizzo quale sistema di pagamento nelle transazioni immobiliari con speciale riferimento alle contrattazioni immobiliari', in Stefano Capaccioni (ed), *Criptoattività, criptovalute e bitcoin* (Giuffrè 2021) 115.

[70] Sabrina Bruno, 'Le initial coin offerings in una prospettiva comparatistica' (2018) VI Riv not 1307; M Simbula, La rivoluzione regolamentare in arrivo negli Stati Uniti e in Europa e la normativa in materia di strumenti finanziari e di tutela dei consumatori, in Stefano Capaccioni (n 69) 260.

[71] Giuseppe Niccolini, 'Gettoni e buoni d'acquisto: ancora una generazione di mezzi di pagamento?' (1978) I Rivista di diritto civile 94.

[72] For cryptocurrencies, the *blockchain* is a widespread and participatory 'financial centre' that does not require an authority to issue and control the currency and its value. The *blockchain*, therefore, locates a 'transaction cadastre' on a decentralised and a-territorial system. At the heart of cryptocurrencies is the idea of eliminating any form of intermediation in order to allow users to communicate peer-to-peer, i.e., by communicating with each other on an equal footing and giving consent for their transactions to be stored on a ledger. A copy of this log is distributed and stored by a computer network composed of 'nodes'. Each 'node' has the information regarding all the operations that have taken place up to that moment and allows conveying the data relating to the transitions made by other users, thereby validating, to some extent, the transitions shared between the various nodes. To sum up, the data are not stored by a centralised registry guaranteed by a central authority but in 'distributed' form, because each of the 'nodes' corresponds to a copy, which minimises the risk of unilateral loss or alteration of data. As for the exchange phase, the validator computers in the network check the conformity of the public key with the private key used to sign the transaction, and also verify that the settlor actually holds the cryptocurrency to be transferred. After validation, the operation will then be recorded as a new block in the chain. The exchange usually takes place either directly or through an exchange, i.e., a third-party platform, which allows virtual currency to be exchanged for traditional currency or other crypto-assets at a certain market price.

[73] See Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing OJ L 156 43. The *rational* of the rule clearly moves in the direction of overseeing the areas of interference with current currencies and the real economy without correctly defining the phenomenon. Recital 10 of the Anti-Money Laundering Directive demonstrates this assumption by stating that 'although virtual currencies can often be used as a means of payment, they could also be used for other purposes and have wider use, for example as a medium of exchange, investment, as a store of value products or be used in online casinos. The objective of this Directive is to cover all possible uses of virtual currencies.' For similar considerations, see Fabio 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 Francesco Fimmanò and Giovanni Falcone (eds), *FinTech* (ESI 2019) 292.

value, but is accepted by natural and legal persons as a medium of exchange and can be transferred, stored and exchanged electronically'.[74] This leads to a negative distinction between virtual currencies and fiat currencies.

According to European legislators, virtual currencies are not the monetary expression of national or supranational authorities. They are not issued or guaranteed by a public authority and do not have the status of money or currency, even if used as a medium of exchange like common traditional currencies. However, a contradiction emerges where virtual currency is denied the legal status of money, even though it is used as a medium of exchange to purchase goods or services. In such a case, it would be conceivable that the EU legislature would not leave room for interpreters to consider virtual currency and fiat money to be equivalent, because the laws of the Member States need to define money.

The Anti-Money Laundering Directive also uses terms such as 'money' and 'currency', one as a synonym of the other, because they are widely used in the laws of the Member States to identify the legal tender currency (the euro) or the foreign currency. In Italian law, for example, the term money occurs in articles 1277 of the Civil Code, 1278 of the Civil Code, 1279 of the Civil Code, 1280 of the Civil Code, 2343 ter of the Civil Code, 2343 quarter of the Civil Code, 2427 of the Civil Code, while the term 'currency' appears mainly in financial legislation. In the German BGB, the term *Währung* refers to the currency (§244), the term Geld, the currency of pecuniary obligation (*Geldschuld*) with foreign currency (§245). Also, in France's *Code monetaire et Financier*, in art. L111-1, the term *monnaie* means the euro, the currency with legal tender in that state.[75]

Only in 2017, when ICOs were broadcast in the media, some countries felt the need to regulate the phenomenon, especially on the initiative of the Financial Market Supervisory Authorities.

The presence of myriad types of cryptocurrencies has also created a 'definition' problem that has led the relevant authorities to direct their efforts towards framing the legal status of the cryptocurrency to which the applicable discipline refers.

Although they are not legal tender, there has also been an attempt to prefer the thesis that cryptocurrencies are a conventional means of payment, an attempt derived above all from the position of the EU Court of Justice in the *Hedqvist* case and, in Italy, of the Revenue Agency since Resolution No. 72/E of 2016.

With this resolution, the tax authority seems to leverage the definition of virtual currency introduced by Legislative Decree No. 90 of 2017 to recognise virtual currencies

[74] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (n 73).

[75] Mario Passaretta, 'Le valute virtuali virtuali in una prospettiva di diritto privato: tra strumenti di pagamento, forme alternative di investimento e titoli impropri' in Stefano Capaccioli (ed), *Criptoattività, criptovalute e bitcoin* (Giuffrè 2021) 97.

'as an alternative payment instrument to those traditionally used in the exchange of goods and services'.[76]

The Italian definition of virtual currency introduced in Legislative Decree no. 231/2007 by art. 1 Legislative Decree no. 90/2017 remains essentially the same after the transposition of the Anti-Money Laundering Directive. Art. 1, letter qq), of Legislative Decree no. 231/2007 defines *cryptocurrencies* as '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 medium of exchange for the purchase of goods and services or for investment purposes and transferred, stored and traded electronically'. Unlike the Anti-Money Laundering Directive, the national law does not establish a monetary *status*, but adds a possible investment purpose for use of virtual currencies.

The fact that the circulation of cryptocurrencies takes place in the vast world of the web with no defined regulatory framework raises many questions, especially their use for potential tax evasion or money laundering purposes.[77]

Currently, we can count over 2000 species of virtual currency, but of these, the best known[78] is *bitcoin*, which is used as a payment method, although it does not have all the characteristics of money. It is an investment instrument,[79] although it has no specific qualification in terms of a financial instrument and its existence relies on a potentially public register. It is also protected and accessible only by those who have the keys. However, there are problems with personal data protection and, more generally, coordination with EU Reg. no. 679/2016 (GDPR) concerning the processing and free movement of personal data that remain public.[80]

Focusing now on how cryptocurrencies work, it can be summarised that the highlights of the life of cryptocurrencies are their creation, storage, and exchange (with other virtual currencies, with goods or services, with NFTs or even with legal tender currencies). Cryptocurrencies are created through a process known as mining, i.e. digital currency issuance.

The activity of *miners*, which is part of the consensus mechanism called *proof-of-work*, consists of generating a *hash* with specific characteristics established by the

[76] Revenue Agency, Dre Lombardia, answer no. 956/2018.

[77] Ermanno Calzolaio, 'La qualificazione del bitcoin: appunti di comparazione giuridica' [2021] Danno e responsabilità 188.

[78] On this, see Andrea Caloni, 'Bitcoin: profili civilistici e tutela dell'investitore' (2019) 1 Rivista di diritto civile 159. See also Andreas Rahmatian, 'Electronic money and cryptocurrencies (bitcoin): suggestions for definitions' (2019) 34(3) Journal of International Banking Law and Regulation 115.

[79] Pursuant to Italy, Legislative Decree no. 58 of 24 February 1998 (Consolidated Law on Finance), art 1(4) '*i mezzi di pagamento non sono strumenti finanziari*'. Nevertheless, the judgment in Tribunale di Verona, 24 January 2017, n 195 enhanced the store-of-value component, which partly characterises *bitcoin*, by framing it in the context of financial instruments, to apply the rules set out in consumer protection and market integrity law. See Mario Passaretta, 'Bitcoin: il leading case italiano, nota a Trib. Verona, 24 gennaio 2017' (2017) Banca borsa e titoli di credito 471.

[80] Cf Simone Calzolaio, 'Protezione dei dati personali (Dir. Pubbl.)' in Dig disc pubb aggiorn (UTET 2017) 594.

blockchain protocol and is usually complex to comply with, requiring elaborate mathematical computations associated with each transaction or block of transactions, which are then shared with the network in exchange for compensation. This compensation depends on the transactions in the block and the number of addresses to which the amount is sent and not on the amount of cryptocurrency sent. It can consist of a *reward* (issuance of new cryptocurrencies) or a *fee (*cryptocurrencies to complete the transaction quickly). This mechanism is, for example, the basis of *Bitcoin*.

It differs from *proof-of-work*, in that so-called *proof of stake* is based on validation rights given to users based on *stake*. Unlike *miners*, validators are called *forgers* or stakes and their task is to verify or validate a transaction without mathematical calculations, while tying up liquidity to guarantee their commitment to carry out the validation correctly and consistently for a fee.

In addition to *mining* and *forging*, cryptocurrencies can be made available to users in other ways. Examples include the *Airdrop*, where *tokens* are made available without consideration (to create a 'community' of *tokens* and increase liquidity); the *Initial Coin Offering (*ICO), i.e. the creation of tokens issued in exchange for cryptocurrencies or legal tender currencies, and finally *minting*, i.e. the issuance of *tokens* without a public or exchange offer which are thus born, so to speak, for their own sake. On the other hand, regarding the circulation of cryptocurrencies, once the procedure for creating one's *wallet* has been completed, the customer's first address will be generated, which he will use to receive or transfer cryptocurrencies.

It should be noted from the outset that *bitcoins* are a set of elements in a transaction and elements of the *script* programming language. What is commonly called a *wallet* or 'portfolio' does not contain any cryptocurrency, only the private keys (hence the name 'key ring') to send transactions, which can be copied by anyone who learns the number sequence.[81]

In strictly technical terms, cryptocurrency is a pair of keys, one private and one public. The first is known only to the rights holder represented by the crypto asset or by a possible delegate. The second is known by all those participating in the system in which it circulates. The information contained in the public parameter – also encoded in the message – is, in fact, the ownership, the value attributed to it and the transaction history.

On the other hand, the private parameter allows transfers or other operations on crypto-assets through cryptographic authentication of the digital signature. However, there are other more complex cryptographic systems, such as multisigs, where control over the digital asset is achieved through multiple digital signatures.

[81] Andreas M Antonopoulos, *Mastering Bitcoin* (O'Reilly & Associates Inc 2017).

Therefore, the legal qualification of virtual currencies requires interpreters to carefully delimit the phenomenon. However, in view of changes in technology, an update is needed to the concepts and terms involved. Part of the doctrine has excluded virtual payment currencies from being considered a newly minted currency (including electronic currency under article 114 bis et seq. of the Consolidated Banking Act), considering that money is only what the State adopts to settle pecuniary debts.[82] In this regard, it has been observed that even setting aside the fact that a public authority does not prefer a virtual currency, one defect in its qualification as a currency would survive in that its monetary function is imperfect.

Money fulfils three functions: expression of a value (unit of account); preservation of purchasing power over time (store of value); and means of payment (or exchange). The first function seems challenging to recognise in cryptocurrencies, as it is compromised by the (still) modest level of economic operators who adopt them, as well as by the volatility of the value on the market and, therefore, of purchasing power.[83]

In light of the considerations made around reinterpreting the concept of 'thing' within the historical period, crypto assets can be brought back within the scope of art. 810 of the Italian Civil Code[84], as an intangible thing, a possible object of law and, therefore, a legal asset in all respects, even if intangible in terms of consistency.[85]

[82] Vincenzo De Stasio, 'Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento' (2018) 6 Banca Borsa e titoli di credito 749; Gianluca Guerrieri, 'I rischi alla circolazione della moneta elettronica' (2014) 5 Le Nuove leggi commentate 1043.

[83] Giovanni Rinaldi, 'Approcci normativi e qualificazione giuridica delle criptomonete' (2019) 1 Contratto e impresa 257; see also Roberto 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.

[84] On the concept of economic good, cf Giovanni Palmiero, *Elementi di economia politica* (Cacucci 2008) 24.

[85] *Contra* Guido Befani, 'Contributo allo studio sulle criptovalute come oggetto di rapporti giuridici' [2019] Il diritto dell'economia 232, believes that the civil regulation of cryptocurrencies should not fall within the scope of art. 810 of the Civil Code, because the semantic ambiguity of the provision would leave ample room for manoeuvre to the questionable sensitivity of the interpreter as to whether or not to include cryptocurrencies among the 'things that can be the subject of rights. If there is to be regulation, it should be left to legislators, who alone have the necessary binding authority to impose a definition of cryptocurrency that is free from any misunderstanding or hermeneutic confusion. While remaining true to the physicalistic concept of 'things', we see that Paolo Luigi Burlone and Riccardo De Caria, 'Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale' (*IBL Focus* 2014) 4, referring to *Bitcoin,* argues that 'it is first and foremost an asset, in the sense made its own and defined by the Civil Code: "goods are things that can be the subject of rights" (Article 810 of the Italian Civil Code). Of course, it will be movable property, and above all, because of its nature without any physical support, it will be an intangible asset'; in the same light, according to Carla Pernice, 'La controversa natura giuridica di Bitcoin: un'ipotesi ricostruttiva' [2018] Rassegna di diritto civile 345 there do not appear to be any theoretical obstacles to bringing Bitcoin back into the operational perimeter referred to in art. 810 of the Italian Civil Code, as a 'new intangible asset'. However, according to a cornerstone of the classic theory of intangible assets, although it is not enshrined in any rule of positive law, the attribution of exclusive rights over all incorporating entities should be considered regulated, in our legal system, 'by a substantially typical system; the content of those rights varies according to the nature of those entities and the interests vested in them [...]. Interests in entities other than property and without legal recognition (direct or analogue) enjoy limited protection and are characterised by the absence of exclusivity.' On this see Zeno-Zencovich (n 29) 460. On this point, Roberto Bocchini, 'Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche' (2017) 1 Diritto dell'informazione e dell'informatica 28, noted that the real caveat of this reconstruction is represented by the circumstance that the attribution of exclusive rights over intangible assets is regulated, in our system, by a principle of strict typicality. On this basis, the road to the qualification of cryptocurrency as a legal asset has only to go through a different conception of the term 'thing'.

According to this reconstruction, payment with virtual currency would be included in the exchange model (Article 1552 of the Civil Code)[86] because the payment would constitute a reciprocal transfer of things or other rights from one contracting party to another. Others, on the other hand, include payment by virtual currency within the scope of services in lieu of fulfilment (Article 1197 of the Civil Code),[87] because the price can only be determined in fiat money.

5 The use of trust for the generational transfer of cryptocurrencies and NFTs

The legal qualification of *digital assets* – and cryptocurrencies in particular – is a complex activity 'at all latitudes'. Interpreters, doctrine and jurisprudence try to frame the phenomenon by resorting to the hermeneutic methods and legal categories of their respective traditions, often with profound differences between *civil law* and *common law* countries.

Inevitably, in the coming years, we will also see interventions by legislators, which are likely to be disparate.

Therefore, identifying rules to apply to digital assets, which are intangible and cannot be placed geographically, is a difficult task.

Concerning the common law[88], it has been noted that 'Digital assets, and cryptocurrencies in particular, do not fit into traditional categories of property as understood by the common law, being neither "choses in possession" ' – as intangible assets – nor ' "choses in action" ' – because, especially with cryptocurrencies, it is not usually possible to identify a person on whom one's right of nature proprietaries can be enforced.

The question then arose as to whether or not *digital assets* were, all things considered, *property*.

Doctrine and progressively consolidating[89] jurisprudence[90] have responded positively[91], defending the duality of *personal property* and believing that the category of *chose in action* could also include such *digital assets*, given its breadth and flexibility.

[86] V Stefano Cerrato, 'Negoziare in rete: appunti su contratti e realtà virtuale nell'era della digitalizzazione' (2018) I Rivista del diritto commerciale 440. Similarly, part of the German literature traces the fulfilment of cryptocurrency back to §480 BGB (*Tausch)*, on the consideration that the fulfilment of an obligation is only possible with fiat money: hence Stefan Omlor, 'Geld und Währung als Digitalisate' [2017] Juristenzeitung (JZ) 754, 763.

[87] Giorgio Gasparri, 'Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?' [2015] Diritto dell'informazione e dell'informatica 445.

[88] Gilead Cooper, 'Virtual property: trusts of cryptocurrencies and other digital assets' [2021] Trusts & Trustees 1, 10.

[89] Cf. *inter alia,* B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(I) 03; Ruscoe & Moore v Cryptopia Limited (in liquidation) [2020] NZHC 728.

[90] *High Court of England* in *AA* v *Persons Unknown, Re Bitcoin* [2019] EWHC 3556 (Comm).

[91] However, they did so 'instinctively', without the nature of the *property rights associated with* digital assets *having yet been exhaustively clarified* ('In trying to ascertain the rights associated with this new form of asset, the law looks

However, a different approach has argued that the advent of cryptocurrencies and all crypto assets is shaking the pre-existing dual model. It is necessary to establish a new class that acts as a *tertium genus* between *chose in action* and *chose in possession*, capable of better combining the characteristics of cryptocurrencies with the proprietary regime.[92] This position was recently accepted by the Law Commission of England and Wales in its report contemplating a new personal property category. Indeed, in the commissioners' view, the characteristics of *chose in action* and *chose in possession* are irrelevant to the nature and functions of crypto tokens.[93]

A fundamental precipitate of qualifying digital assets as property is that they can be the subject of trust.

Recognising that *digital assets* can be the subject of trust opens the door to using the estate planning tool.

An immediate advantage is related to the fact that, by entrusting the custody of digital assets (crypto in particular) to a professional trustee by *inter vivos* deed, the problem related to the delivery of credentials (IDs / Passwords / private key) that we have seen afflicting devolutions *mortis causa* is solved.

Having ascertained that cryptocurrencies can be the subject of trust, the legal literature has questioned whether a trustee must invest in virtual currencies.

'The Trustee Act 2000 requires trustees to consider standard investment criteria, including the need for diversification of the trust's investments, to the extent appropriate to the circumstances of the trust. This is framed as a duty to consider diversification, not a duty to diversify. Until recently, and perhaps will be for some time to come, cryptocurrencies have been too volatile and speculative to be considered a reliable, or even plausible, investment. However, cryptocurrencies are becoming increasingly "reputable", and it is not hard to imagine a future, possibly not too far away, where a trust, especially a suitably sized one, could reasonably consider including at least one element of exposure to a potentially valuable investment. [...] There is no reason why a trust should not include a very high-risk investment in a balanced

to analogies; shares in a company; promissory notes and bills of exchange; safety deposit boxes (and their keys); Goodwill; patents; the list could be continued. But none of these analogies is exact').

[92] In *AA* v *Persons Unknown*, the Supreme Court noted on p. 21 how: 'Prima facie, *there is a difficulty in treating Bitcoins and other crypto currencies as a form of property: they are neither chose in possession nor are they chose in action. They are not choses in possession because they are virtual, they are not tangible, they cannot be possessed. They are not choses in action because they do not embody any right capable of being enforced by action. That produces a difficulty because English law traditionally views property as being of only two kinds, choses in possession and choses in action*'.

[93] See *Law Commission Final Report: Digital Assets. Presented to Parliament pursuant to* section *3 (2) of the Law Commissions Act 1965. Ordered by the House of Commons to be printed on 27 June 23*. In particular, at *Chapter 3* , '*A Third Category of thing to which personal property rights can relate*', 33 ff.. Cf. Giulia Bazzoni, 'I riflessi del regime proprietario delle criptovalute sul trust (ByBit Fintech Limited v Ho Kai Xin, 25 July 2023)' (2024) 1 *Trusts e attività fiduciarie* (forthcoming).

portfolio. In the case of trustees of UHNWI settlements, there may be opportunities to achieve significant gains from relatively modest investments'.[94]

Suppose it has been established that a trustee can hold cryptocurrencies. In that case, it should be argued that he must invest in cryptocurrencies to diversify the trust fund and avoid possible liability for not taking opportunities.

As a result, the trustee could invest in cryptocurrencies. On the other hand, there is an issue of risk. In fact, disputes could well arise from the beneficiaries of the trust because, due to the volatility of cryptocurrencies, the trust fund could change in quantitative terms.

At this point, it becomes essential that trusts are set up expressly to hold crypto in the presence of specific regulations, or that the trust regulation contemplates the possibility of having cryptocurrencies within them.

Given the development of technology, one might wonder whether a world in which smart contracts will replace trustees is conceivable and whether intelligent contracts can play a role in the trust industry.

Smart contracts, applied to basic contracts, are the future; conversely, it is difficult to imagine that smart contracts can replace trustees or that bright deeds can be crystallised on the blockchain.

The trustee's job is, first and foremost, to recognise the changing reality of the world and to exercise, in the light of it, his fiduciary office in the interest of the beneficiaries, balancing the various needs that arise.

This is not the same as taking advantage of some of the immutability features of the blockchain to give certainty to trust deeds and the book of events instead.

6 Digital Inheritance

In this context, the dialogue between two illustrious scholars, Natalino Irti and Emanuele Severino,[95] on the relationship between law and technology appears, from the dual perspective of the jurist and the philosopher, to be of considerable interest. From it emerges, from the jurist's perspective, the positivistic conception of law made up of norms having exclusively procedural validity, but not truths of content, within which ideological, political or economic propositions must be translated in order to be adequate. The same technique, Irti argues, would have the same abstraction and therefore would be unable to answer the fundamental questions of the law.

From the philosopher's perspective, on the other hand, technology is destined to become the regulative principle of all matter, the will that regulates every other will.

[94] Gilead Cooper, 'Virtual property: trusts of cryptocurrencies and other digital assets' [2021] Trusts & Trustees 1, 10.
[95] Natalino Irti and Emanuele Severino, *Dialogo su diritto e tecnica* (Laterza 2001); Vittorio Frosini, *Il diritto nella società tecnologica* (Giuffrè 1981) 202; Giuseppe Corasaniti, *Il diritto nella società digitale* (Franco Angeli 2018).

Starting from the basic idea that technology does not, in essence, have exclusionary ends, but rather aims for infinite growth in power, Severino goes so far as to affirm that it reveals its concreteness since it is the form of the natural production of ends, which contributes to the indefinite expansion of the scientific and technological apparatus. Irti, however, believes that technology, as a 'form of will be aimed at achieving non-exclusive ends, would exclude all ends that are contrary to one's infinite capacity to achieve ends'.[96]

It is undeniable, however, that abstract, ex ante regulation of disruptive innovative phenomena like cryptocurrencies and crypto assets is challenging.

As we have seen, this difficulty arises from the awareness that the theory of goods is not exhausted in the theory of rights in rem or in that of property and that it is not always easy to identify the characteristics of every possible good with those of goods subject to the right of property, much less is it possible to exclude utilities that are not suitable for subjective proprietary (or at least real) situations from being defined as goods.

Until a few years ago, one of the controversial aspects of the circulation of trusts in our legal system was the difficulty of identifying a case that could support a transfer of ownership, hence the issue of the admissibility of functional ownership with restricted use different from the provisions of under Art. 832 of the Italian Civil Code. Assuming the trustee had fiduciary ownership without the power to enjoy and dispose of it freely, the trust would also violate the principle of typicality and the *numerus clausus* of rights in rem. Legal theory had to put forward several arguments supporting the so-called deconstruction of the dogma of proprietary absoluteness and *perpetuitas*.[97]

Although most legal theory agrees with defining virtual currencies as intangible assets, i.e. art. 810 of the Civil Code, according to which 'goods are things that can be the subject of rights', the proposed reconstruction presents some critical issues.

One argument to the contrary is of a theological nature[98] and is based on the limited number of assets referred to in Article 810 of the Civil Code, the extension of which must be established by legislators. On this, it should be noted that virtual currencies are considered only in the anti-money laundering discipline because they are a possible

[96] Giancarlo Montedoro, *Il diritto pubblico tra ordine e caos I pubblici poteri nell'età della responsabilità* (Cacucci 2018).
[97] Cf Antonio Gambaro, 'I trusts e l'evoluzione del diritto di proprietà', in Ilaria Beneventi (ed), *I* Trusts *in Italia oggi* (Giuffrè 1996) 57; Antonio Gambaro, *Il diritto di proprietà* (Giuffrè 1995) 629; Umberto Morello, 'Tipicità e numerus clausus dei diritti reali', in Umberto Morello and Antonio Gambaro (eds), *Trattato dei diritti reali* (Giuffrè 2008) 67; Ermanno Calzolaio, 'La tipicità dei diritti reali: spunti per una comparazione' [2016] Rivista di diritto civile 1080. Cf Michele Graziadei, 'Trust, confidenza, fiducia', in Richard H Helmholz and Vincenzo Piergiovanni (eds), *Relations between the ius commune and English law* (Rubettino 2009) 225.
[98] Cf M Costantino, 'I beni in generale', in Pietro Rescigno (ed), *Trattato di diritto privato* (UTET 1982) 13; Oberdan Tommaso Scozzafava, *I beni e le forme giuridiche di appartenenza* (Giuffrè 1982) 422; P Liberanome, 'Criptovalute tra anarchia e difficili tentativi di regolamentazione' in Fimmanò and Falcone (n 73) 426.

vector of illicit proceeds or for the financing of terrorism, so it follows that there could be no regulatory recognition of them as assets.

The second argument, which is literal, points out that only things that can be the object of rights can be goods. Furthermore, things are, by their very nature, corporeal.[99] Identifying a bit circulating in the ether in the impression created in a silicon memory is a noticeable stretch, since the object of circulation is not the physical medium but what is read through it.[100]

The non-admission of virtual currencies as intangible assets means that the hypothesised rules of exchange (Article 1552 of the Civil Code) are not applied to their exchange. However, the exchange should be qualified as a contract of sale if the parties establish the consideration in conventional currency.[101]

For the same reason, the use of cryptocurrency in the payment system cannot always be considered as *datio in solutum*. We can only speak of *datio in solutum* if the payment with a virtual unit of account takes place instead of the payment in legal tender, and therefore in euros. Otherwise and therefore if virtual currency had been the agreed tender from the beginning, there could be no substitution with legal currency, and the consent of the creditor who consented to it from the beginning would not make sense.[102]

Having made this necessary digression, 'digital assets' has now become an expression in current use, even in ordinary language, defining complex goods and legal relationships as digital, because they are connected to the use of technological devices and the internet. A digital asset is not only identified with virtual currency or cryptocurrencies in general; this type of asset is only one of the possible digital assets that could be the subject of trust. It is customary to refer to this macro-category as pure digital assets and those that, in the short term, will probably be the most thorny digital assets to be processed, i.e. personal data in the strict sense because personal data, which can be the elementary identifying one, represents, at present, a rather sought-after bargaining chip and the databases that contain personal data have an enormously increasing economic value.

The definition of digital asset was born from reflection in the criminal field, but has recently found an express regulatory reference in our Consumer Code, as most recently amended following the transposition of the twin directives in 2019, specifically Directive

[99] See Roberto Bocchini, 'Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche' (2017) 1 Diritto dell'informazione e dell'informatica 27, 33.
[100] Gianfranco Liace, 'I titoli al portatore (artt. 2003-2007)', in Piero Schesinger, *Commentario* (Giuffrè 2017) 46.
[101] Gastone Cottino, 'Riporto Permuta' in Antonio Scaljoa and Giuseppe Branca, *Commentario* (Zanichelli 2012) 80, n 5; Sarah Green, 'Cryptocurrencies: The Underlying Technology, Cryptocurrencies' in Sarah Green and David Fox (eds), *Public and Private Law* (OUP 2019) 68.
[102] Sarah Green, 'Cryptocurrencies: The Underlying Technology, Cryptocurrencies' in Sarah Green *Cryptocurrencies in Public and Private Law* (Oxford 2019) 29; Mario Passaretta, 'Il problema della qualificazione giuridica delle valute virtuali. Il difficile approccio regolamentare', in Stefano Capaccioli (ed), *Criptoattività, criptovalute e bitcoin* (Giuffrè 2022) 99.

2019/771 which has the merit of having provided an initial definition for digital content and digital services.

The revolution in decentralised systems, commonly called "Web 3.0", relies on the good quality of the data stored on the blockchain and not necessarily on a financial authority that verifies and validates the individual transaction.

As for the macro-category of pure digital assets, the management, conservation, ownership, and transmissibility of digital inheritance through trusts is one of the most emblematic wealth-planning solutions.

The topic of digital inheritance, with its somewhat uncertain contours, has fascinated lawyers in recent years, including the succession of cryptocurrencies as the digital "asset" par excellence. In this matter, four general principles of inheritance applicable to cryptocurrencies have been developed.

The first principle is that of the 'analogic analogue', where the digital novelty is approached by trying to bring it back to an analogue paradigm that is in some way already regulated, such as bitcoin to cash.[103]

A second principle relates to the transnational extension of the value of the principles underlying decisions taken under the government of foreign legal systems.[104] An example is the well-known German case involving a request for access to Facebook by the parents of a young suicide victim. Three principles were established from this: the contents of the account are subject to inheritance; any contractual clauses are non-binding, as they are abusive; and, finally, the dissemination of information does not violate the GDPR.[105]

A third principle concerns the centrality of the electronic document and the distinction, also legal, between the medium and document. Similarly, when referring to cryptocurrency in cases of succession, it must be clarified that the support (*hardware wallet*) events are indifferent to those of the document it contains.

The last principle of digital inheritance is the strict distinction between legal assets and digital access to analogue assets.[106]

It is understood that it is different to have cryptocurrencies included in funds that invest in cryptocurrencies in various ways, have them with intermediaries, or directly hold the private keys for their movement. There is also a diversity of cryptocurrencies, so much so that bitcoins are not the same as NFTs. Therefore, people's digital assets are assets whose solutions must be identified individually.

[103] Carla Pernice, *Digital Currency e obbligazioni pecuniarie* (ESI 2018); Carla Pernice, 'La controversa natura giuridica di Bitcoin: una ipotesi ricostruttiva' (2018) 1 Rassegna di diritto civile 333; Carla Pernice, 'Crittovalute e Bitcoin: stato dell'arte e questioni ancora aperte', in Francesco Fimmanò and Giovanni Falcone, *FinTech* (ESI 2019) 419; Mario Passaretta, 'Bitcoin: il leading case italiano' [2017] Banca borsa e titoli di credito 471.
[104] Giuseppe Marino, 'La "successione digitale"' [2018] Oss dir civ e comm 193.
[105] Maddalena Cinque, 'L' "Eredità digitale" alla prova delle riforme' (2020) 66(1) Rivista di diritto civile 85,87.
[106] Remo M Morone, 'Le problematiche successorie e di donazione nelle criptovalute' in Stefano Capaccioli (ed), *Criptoattività, criptovalute e bitcoin* (Giuffrè 2021) 139.

7 Transmission of virtual currency and trust

One of the essential themes of digital inheritance and the succession of cryptocurrencies relates to the complex issues concerning material *post-mortem* apprehension. Access to cryptocurrencies can be difficult for three different reasons. First, it is an entirely anonymous universe where the cost of opening a new account is zero. Therefore, it is suggested that different addresses be used for each transaction, creating a clearer multiplicity of different purchase and spending centres. These different accounts can be grouped into so-called hierarchical-deterministic wallets or managed indirectly through access credentials to web wallets. These two aspects, created technically to simplify access, perhaps conceptually and legally, complicate it.

In addition to all this, there are no official registers in the Italian legal system, which instead have historically been in force for real estate and, indirectly, through the small and controlled number of authorised intermediaries, also for financial wealth, certainly does not help the heirs of cryptocurrencies, taking into account the fact the reasons for confidentiality and security that underpin the prudence suggested in the storage of private keys. They make it even more difficult for the beneficiaries of the succession to discover their existence, at least until appropriate measures are taken.

Finally, the physical media on which the access keys are contained have a physical inheritance legal history that is potentially different from that of the digital assets. The beneficiary, of course, must then be entitled legally and, therefore, must be either an heir or a legatee of the corresponding sum, because the executive aspect is not sufficient in Italian law for the transfer of wealth.

Therefore, it is not enough for those who hold the private keys of a bitcoin wallet, for example, to worry only about the transfer of the code to another person or the beneficiary of a trust; there must also be a legal transfer of ownership of that asset.

The ownership of the asset can be transferred to the trustee, as well as the availability of the key for the generational transfer. In this case, however, they should be discontinued in the declaration of succession, if it is considered appropriate that the latter should be submitted.

Some scholars argue that the inheritance tax and the compilation of the inheritance declaration on crypto assets should not be carried out based on the presumption of article 9 of legislative decree 346/1990, which establishes the exemption for money present in the inheritance. In light of this, it is believed that it is not wrong to argue that if the tax administration espouses the idea of considering cryptocurrencies as foreign money; perhaps inheritance tax should not be applied, falling within the presumption. This, however, does not mean that it is not cheaper to pay a 4% inheritance tax than 26% capital gains. It would also be cheaper, since inheritance is the basis for calculating capital gains according to current tax legislation.

What is certain is that the situation will only change after the entry into force of the mica (markets in crypto-assets) regulation scheduled for the middle of next year, which, with its 126 articles, will replace the current existing fragmented national frameworks about crypto assets and will introduce specific rules for their offer and marketing as well as regulate the role of esma – the European securities and markets authority – and the eba – the European banking authority.

In order to facilitate the management and planning of assets, and therefore also the succession of digital assets, the ideal arrangement is one in which the data of the digital assets are kept secret until the time of death, considering that they are easily updated in the meantime, since the digital asset par excellence is very fluid. Several solutions have been proposed, but indication of the credentials of the keys in the will remains somewhat risky, because the will, although secret, still needs to be published. Therefore, this highlights a significant limit to confidentiality.

In this case, the indication and storage of documents in safe deposit boxes (or, more appropriately, the seed of the deterministic hierarchical datasheet or at least a hardware wallet) could be an efficient solution, although inconvenient from a practical point of view, even if tempered by techniques that allow multiple accesses, including perhaps access in the safe deposit box and access to the outside. In the case of a bequest, the legal figure is the “legacy of a thing to be taken from a certain place” under art—655 of the Italian civil code.

It is clear, however, that the reasons for confidentiality and security underlying the particular prudence suggested in preserving private keys prevent the beneficiaries of the succession from discovering their existence if appropriate measures are not taken.

If the settlor can facilitate access to cryptocurrencies for the unaccustomed heir while maintaining control of his wallet, more significant difficulties could arise for the beneficiaries' access to the assets.

In order to facilitate enforcement, the settlor could make use of a *post-mortem exequendum* mandate, i.e., he could appoint a third party to perform certain operations upon his death, such as handing over one of the private keys to the beneficiary or arrange for the admission on the blockchain a transaction (possibly already signed by the settlor) that "fills" the address where the beneficiary is in possession. Some have criticised this mechanism on the grounds that it could overlap with the prohibition of inheritance agreements. In fact, as the doctrine has had the opportunity to explore, it is a primarily theoretical problem, considering that if the mandate is adequately and legitimately constructed, death is only the end of fulfilment and is extraneous to the causal mechanism.

It is also possible to resort to using smart contracts such as, for example, the so-called smart contracts. Dead man switch: the wallet is loaded with a sum and periodically checks whether the settlor is still living. Prolonged inactivity would result in a transfer of the sums to another wallet whose keys are automatically communicated to

the beneficiary. Alternatively, it can resort to the so-called multi-sig wallet, which requires a movement of multiple access keys. This would be a key held by the settlor, another by the trustee and a third provided in advance to the beneficiary, which would give them access at the appropriate time.

8 Conclusion

Assets in the digital age are composed of movable and immovable assets and different entities that, although material, are characterised by an additional characteristic or are preferable to a specific digital context determined by technological evolution.

From a legal point of view, new needs are emerging to balance opposing values and the need to rethink many traditional categories.

The importance of regulation is also evident for the differential treatment that is inevitably required when there is a trust that has as its object digital assets during the existence of its owner and trusts that will have to deal with managing these assets after the owner's death.

For example, in some jurisdictions, including California, interesting laws have already been enacted on the management of digital assets through trusts, but only the time after the death of the owner of these assets has been considered. At the same time, it is known that the problem already exists for the deed of trust alone of these 'new goods', in the absence of an adequate regulatory framework. The tax codes and the most critical CEOs of some professional trust companies, especially in Switzerland, have strongly emphasised the need for training of the trustee on this new category of assets that are characterised above all by a lack of stability in their value and Fintech, considering the obligation for trustees to diversify the assets entrusted to it under management.

The real problem, however, lies in the possibility of accessing digital assets on the death of the owner because, in this case, a whole series of complex actions collide, including, for example, the contract that the individual signs when accessing digital assets, more or less consciously, with the large server providers. In most cases, these contracts provide for the impossibility of accessing personal data, which are also considered digital assets that can be accessed with personal credentials, making it difficult for heirs to take over these positions, which can only be overcome by order of the judge or in other even more complex ways.

Such situations that have given rise to multiple rulings, especially for possible conflicts with regulations put in place to protect the consumer; contractual models that raise applicable legal issues, precisely because they are prepared unilaterally by large digital companies that are based in places other than the one where the service is provided.

Inevitably, doubts arise about the lawfulness of access to such digital assets, both at the exchange and at the wallet provider, when confronted with the provisions of Articles 93 and 23 of the Copyright Act about the powers that are vested in the relatives over the copyright of the deceased and Art 2 *terdecies* GDPR to the privacy rights of the deceased.

Similar judgments have recently been made in Italy. Indeed, some very recent rulings, including in the Courts of Milan[107] and Bologna[108] in 2021 and, most recently, the Court of Rome[109] in 2022, have reiterated that, according to Art. 2 *terdecies* of the Privacy Code, denial of access to the personal data of the deceased user is entirely unjustified, where the conditions established by law are met.

The mere loss of the wallet holder's private key will likely prevent future access to their heirs. The same could be said for NFTs, especially at a time when, with the end (or almost) of the era of mistrust, Italian practice is experimenting with increasing curiosity and liveliness with the many functions that the trust can perform and is experiencing the many benefits that this, and not others, can provide to operators.

Among the many application developments being cultivated, there is also the use of trusts as a vehicle for private cultural heritage, which expresses two possible purposes: the community's destination and the management of generational transitions. This, however, could also be applied to cultural heritage held by Public Administrations, an area in which the oft-mentioned cultural gap emerges overbearingly.

It is argued, therefore, that the complexity of the knowledge required for adequately managing such portfolios demands a suitable activity on the part of the post-mortem agent, the executor or even the trustee, which could be carried out by a company specialising in digital inheritance. However, it must be evident that, in some cases, the reason for decentralisation is to be found precisely in the lack of trust in the intermediary.

However, a new enhancement of the role of the guardian could be envisaged, where he or she would fill the hybrid knowledge required by the digital innovation that increasingly pervades the present day, so much so that the new generations are more likely to be owners of this type of asset.

Another fundamental point of reflection is represented by the best practices that should be followed in the presence of personal digital assets. Indeed, it is preferable to draw up an inventory to have knowledge and awareness of digital assets.

[107] Tribunale di Milano, Sez I, Ord 10 February 2021 <https://onelegale.wolterskluwer.it> accessed 25 March 2024.
[108] Tribunale di Bologna, Sez Civ I, 25 November 2021 <https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2022/01/20/Tribunale%20di%20Bologna.pdf> accessed 25 March 2024.
[109] Tribunale di Roma, Sez VIII, Ord 10 February 2022 <https://rivistapactum.it/app/uploads/2022/08/1.-Trib.-Roma-sez.-VIII-ord.-10.02.2022.pdf> accessed 25 March 2024.

Secondly, it is essential to turn to experienced professionals who will undoubtedly recommend a form of management and planning for digital assets through instruments *inter vivos*, thinks of the trust, with the consequent possibility of segregating these assets and having the management of them through the instrument itself; *mortis causa*, such as a will drawn up according to precise indications, which would allow the expression of testamentary instructions for the intergenerational transfer of these assets, on the death of the owner.

The horizon that the jurist sees is not an exclusionary alternative between the real and virtual of the assets conferred in trust, but an inclusion of all the manifestations of human autonomy of the conceptual innovation of cryptocurrencies that consequently requires new interpretative schemes to be able to approach and fully understand, including in relation to historical elements. Jurists, particularly civil lawyers, are called on to become perceivers of the historical line in which we place ourselves and try to order it.[110]

The slow adaptation of the regulatory framework to the dynamics of the blockchain, in the sense of strengthening the protection of the rights of the protagonists of 'Web 3.0', calls for a more excellent balance of ownership relationships between the parties to avoid loss of trust in the digital context. The risk, therefore, is that the new ownership dimension, which was supposed to be the protagonist of the revolution caused by crypto assets, will end up bending to interests that are not always worthy, which seem to find an ideal ecosystem in the metaverse, thus reviving the historical distrust of trusts.

There is a risk that the use of virtual currency conceals illicit transactions aimed at carrying out money laundering conduct, thus forcing the interpreter to question the completeness of the measures regulated in the fifth Anti-Money Laundering Directive for adequate protection. This foreshadows a process of reorganisation and modernisation of the rules, for which European Union legislator have a fundamental consultation role to play.

Today, more than ever, 'ordering, the lofty task of the jurist, does not mean immobilising, crystallising, fixing in closed systems, in fossilising hierarchies. Today, ordering is a bet that the jurist plays not only on the past and the present but also (and above all) on the future. Today, rethinking the classical categories on the part of the civil lawyer is a commitment that formally invests his mission as a jurist, even before a cultural need'.[111]

[110] Michele Lobuono, 'Nuovi beni e forme di appartenenza' in Capobianco, Perlingieri and D'Ambrosio (n 2) 17, 25.
[111] Paolo Grossi, 'Il diritto civile alle soglie del terzo millennio. Una postfazione', in Francesco Macario e Michele Lobuono (eds), *Il diritto civile nel pensiero dei giuristi* (Giuffrè 2010) 422.

*Ilaria Saretto**

DISPUTES FROM COMMERCIAL SPACE ACTIVITIES

Potentialities and Hurdles of Investor-State Dispute Settlement

Abstract:
Outer space is the "part of the universe which is simultaneously beyond the airspace of planet Earth and accessible to human activity".
The recent decades have seen significant developments in the commercial activities carried out in outer space as well as an increasing diversification in the actors engaging therein. In this context, private investment is on the rise and this trend is expected to continue. With more companies and entrepreneurs exploring opportunities in space exploration, satellite deployment, asteroid mining, space tourism, and other space-related activities, it has become of the utmost importance to establish a consistent legal framework for private actors in outer space. This is even more so considering that their increasing presence in the space industry is likely to result, in the near future, in disputes between said actors and States operating in outer space, the resolution of which needs clarity regarding the applicable mechanisms.
Against this backdrop, International Space Law as the "part of existing legal systems on Earth which relates to outer space" does not seem capable of offering, at the state of play, sufficient protection to private investors engaged in space-related activities. On the contrary, International Investment Law has the potential to establish a structured framework for a rule-based system that promotes and maintains private investment flows in outer space.
Starting from the above premises, the present work investigates the applicability of International Investment Law to private investments made in the context of commercial space activities and, a fortiori, of Investor State Dispute Settlement, as a dispute settlement mechanism developed within the frame of the above body of law, to conflicts arising in outer space between private investors and States. The purpose is to highlight that not only do investments in outer space fulfil the requirements to be granted international investment protection but also that the rationale behind International Investment Law justifies its extension to encompass such investments.

JEL CLASSIFICATION: K30, K33

SUMMARY:

* Graduate in law from the University of Turin.

Investments in Outer Space: Can a Territorial Nexus be Construed? - 3.2.1 Theories Related to Jurisdiction: The Registration of the Space Assets as an Indicator of the Existence of a Territorial Nexus – 3.2.2 Possibly Relevant Factors Beyond the Registration of the Space Assets - 4 Conclusions: The Possible Role of Investor-State Dispute Settlement in Outer Space Activities

1 Introduction: the commercialisation of outer space

I don't think the human race will survive the next thousand years, unless we spread into space. There are too many accidents that can befall life on a single planet. But I'm an optimist. We will reach out to the stars.

Stephen Hawking

Outer space is the "part of the universe which is simultaneously beyond the airspace of planet Earth and accessible to human activity"[1].

Traditionally, outer space has been the domain of States which have undertaken missions of exploration since the second half of the 20th century. Nowadays, the number of actors engaged in space-related activities is becoming all the more diversified. In fact, the recent years have seen a rapid growth in the space industry leading to the emergence of new activities.[2] This is due to the discovery and implementation of cutting-edge technologies, as well as the continuous commercialisation of outer space, which increasingly involves private enterprise in activities of space exploration, utilisation, and exploitation for profit.[3]

In this context, private investment in outer space is on the rise, and this trend is expected to continue.[4] With more companies and entrepreneurs exploring opportunities in, *inter alia*, satellite deployment, asteroid mining and space tourism, it has become of the utmost importance to establish a consistent legal framework for private actors (and the regulation of their investments) in outer space.[5]

[1] Vladlen S Vereshchetin, 'Outer Space' in the *Max Planck Encyclopedia of Public International Law. Vol VII* (Oxford University Press 2012).

[2] Guglielmo S Aglietti, 'Current Challenges and Opportunities for Space Technologies' [2020] Frontiers Space Technologies <https://www.frontiersin.org/articles/10.3389/frspt.2020.00001/full> accessed 8 March 2024.

[3] See Anthony L Velocci, Jr, 'Commercialization in Space: Changing Boundaries and Future Promises' (2012) 33(4) Harvard International Review 49.

[4] See European Space Policy Institute, 'ESPI Report 85 - Space Venture Europe 2022 - Full Report' (May 2023, ESPI) <https://www.espi.or.at/reports/space-venture-europe-2022/> accessed 8 March 2024. According to the report, from 2014 onwards, 482 private investment deals involving European space start-ups, for a total amount of EUR 2.9 billion have been recorded. In this context, 2022 alone accounted for 35% of all investments since 2014 and represents more than the total invested from 2014 to 2019.

[5] Sergio Marchisio, 'Space Law and Governance' (10th United Nations workshop on Space Law, Vienna, 5-8 September 2016) 3. On the importance of private actors in the context of the NewSpace Economy see Peter van Fenema 'Chapter 7: Legal aspects of launch services and space transportation' in Frans G von der Dunk and others (eds), *Handbook of Space Law* (Edward Elgar Publishing 2015) 446 and, John Adolph, 'The Recent Boom in Private Space Development and the Necessity of an International Framework Embracing Private Property Rights to Encourage Investment' (2006) 40(4) International Lawyer 961, 961-962. On the notion of space tourism see Erik Seedhouse, 'Space Tourism', *Encyclopedia Britannica* (2023) <https://www.britannica.com/topic/space-tourism> accessed 8 March 2024. In this regard it should be noted that, private agencies are offering private orbital and suborbital flights. By way of example, the two main

This is all the more so considering that the growing presence of private actors and rising number of stakeholders in the space industry is likely to result, in the near future, in disputes between said actors and States operating in outer space. In this context, alongside the disputes arising from the regular conduct of activities in outer space, disputes could also arise out of outer space collisions which are expected to become more and more frequent. The cause is to be attributed to two intertwining factors: on the one hand, the increasing volume of space traffic; on the other hand, the Low Earth Orbit (LEO)[6] getting saturated with space objects and space debris, that is the set of "non-functional, artificial objects, including fragments and elements thereof, in Earth orbit or re-entering into Earth's atmosphere"[7].

Evidently, the settlement of the abovementioned disputes in the outer space scenario necessarily requires enhanced clarity as per which resolution mechanisms are available to private actors and to what extent they can be resorted to.

Against this backdrop, International Space Law as the "part of existing legal systems on Earth which relates to outer space"[8] does not seem capable of offering, at the current state of play, sufficient protection to private investors engaged in commercial space-related activities.[9] This holds true from both a substantial and a dispute

companies active in the context of suborbital space tourism are: Virgin Galactic and Blue Origins, the latter being a privately-owned space company primarily financed by Amazon's founder, Jeff Bezos. As far as orbital flights are concerned, SpaceX is the leading company in the market.

[6] In this regard, note that there are three different orbits where satellites can be located: Low Earth Orbit (LEO), Medium Earth Orbit located at 26,560 kilometres from the centre of the Earth (MEO) and Geostationary Orbit located at 42,164 kilometres from the centre of the Earth (GEO). For further details on the matter see 'Catalogue of Earth Satellite in Orbit' (*NASA Earth Observatory*, 4 September 2009) <https://earthobservatory.nasa.gov/features/OrbitsCatalog#:~:text=There%20are%20essentially%20three%20types,orbit%2C%20and%20low%20Earth%20orbit> accessed 6 March 2024.

[7] On the definition of space debris see 'FAQ: Frequently asked questions', European Space Agency (ESA) <https://www.esa.int/Space_Safety/Space_Debris/FAQ_Frequently_asked_questions> accessed 28 February 2024. For further details of perspective disputes in outer space see Gérardine Meishan Goh, *Dispute settlement in international space law: a Multi-door Courthouse for Outer Space* (Martinus Nijhoff Publishers 2007) 3 and Tereza Pultarova, 'Space Debris from Russian Anti-Satellite Test Will be a Safety Threat for Years' (SPACE.COM, 16 November 2021) <https://www.space.com/russia-anti-satellite-test-space-debris-threat-for-years> accessed 8 March 2024. Additionally, disputes between private actors and states could arise from the conduction of government run anti-missile tests. By way of example, in November 2021 Russia carried out anti-missile tests with the purpose to defunct the Cosmos 1408 satellite. However, the satellite broke apart into at least 1,500 trackable fragments which resulted in the formation of space debris that threatened to collide the International Space Station and SpaceX's Starlink Satellite.

[8] Bin Cheng, *Studies in International Space Law* (OUP 1997) lxi.

[9] Notably, International Space Law combines different sources of various origins, aiming to grant humanity the use and exploration of outer space without discrimination. While it initially emerged as a branch of Public International Law, consisting of treaties and soft law instruments, governing the behaviour of States in their inter-se relations, as time progressed, International Space law has expanded to include domestic laws and regulations. This notwithstanding, International Space Law is, to date, still largely based on five universal multilateral treaties which were negotiated within the framework of the United Nations Committee on the Peaceful Uses of Outer Space between 1960 and 1980, the UN Space Law Treaties. These are known as: Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 27 January 1967, 610 UNTS 205 (entered into force on 10 October 1967) [Outer Space Treaty]; the Agreement on the Rescue of Austronauts, the Return of Austronauts, and the Return of Objects Launched into Outer Space Apr. 22, 1968, 672 UNTS 119; the Convention on International Liability for Damage Caused by Space Objects, 22 March 1972 961 UNTS 187; the

resolution perspective. In fact, it is under debate not only whether commercial space-related activities fall under the scope of application of International Space Law but also whether private actors, including private investors, can enjoy the status of subjects of International Space Law at all.[10] *A fortiori*, it is also not settled yet if private actors can bring claims under the International Space legal framework which, in any case, lacks an established dispute resolution mechanism and, to date, operates within a fragmented patchwork.[11]

It follows that, as International Space Law appears to be unequipped in providing safeguards for private investors and, consequently, in supporting the needs of the continuously evolving space industry,[12] it either evolves or, and in any case in the meanwhile, becomes necessary to turn to other branches of International Law.

In this regard, International Investment Law, the branch of International Law which, together with Domestic Investment Rules, governs the protection of foreign investment, comes into mind first.[13] In light of its structure and tools, it has been attracted attention as a structured, rule-based framework equipped with an effective dispute settlement mechanism, capable of fostering and sustaining private investment in outer space.[14]

Convention on the Registration of Objects Launched into Outer Space Jan 14 1975 1023 UNTS 15 [Registration Convention] and Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, May 12, 1979, UNTS 1363 (entered into force on 11 July 1984) [Moon Agreement]. Notably, these treaties do not address the behaviour of a Contracting party towards another Contracting Party's investments or nationals' investments.

[10] In this regard see Christina Isnardi, 'Problems with Enforcing International Space Law on Private Actors' (2020) 58 Columbia Journal of Transnational Law 489, 499-512. Indeed, it is not definitely settled whether private entities operating in outer space can be granted the status of subjects of International Space Law and therefore, whether they are recipients of the rights and obligations established thereof. Notably, as International Space Law lacks any precise indication as per whether private entities operating in outer space can enjoy the status of subjects, one may refer to Public International Law within whose framework scholars generally uphold the view that non-governmental entities and multinational corporations are empowered with rights and encumbered with obligations at the international level.

[11] Mahulena Hofmann and PJ Blount 'Space Law Disputes' *the Max Planck Encyclopedia of Public International Law* (OUP 2015) 1.

[12] See Peter Malanczuk, 'Investment Protection of Commercial Activities in Space: Treaties, Contracts, Licences, Insurance, Arbitration' (2018) 19 Journal of World Investment and Trade 951.

[13] On the recognition of International Investment Law as a branch of International Law, see Rudolf Dolzer, Ursula Kriebaum and Christoph Schreurer, *Principles of International Investment Law* (3rd ed, OUP 2022) 19. Additionally, Peter T Muchlinski, Federico Ortino and Christoph Schreuer (eds), *The Oxford Handbook of International Investment Law* (OUP 2008) 6; Valentina Vadi, P*roportionality, Reasonableness and Standards of Review in International Investment Law and Arbitration* (Edward Elgar Publishing 2018) 4; Cristina-Elena Popa Tache, *Introduction to International Investment Law* (ADJURIS - International Academic Publisher 2020) 14. On the definition of International Investment Law as the branch of law covering foreign investments, see Sarah M Alshahrani, 'What Should We Know About the Origins of International Investment Law?' (2020) 48 International Journal of Legal Information 122, 123. Additionally, International Law Commission 'Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law' (United Nations Publications 18 July 2006) <https://legal.un.org/ilc/documentation/english/a_cn4_l702.pdf> accessed 8 March 2024. The report is worth noting as it defines international investment law as the specialised field of "general international law" dealing with foreign investment.

[14] On the application of International Investment Law to space-related investments see *inter alia* Christopher Greenwood, 'Oceans and Space: Some New Frontiers for International Investment Law' (2018) 19 Journal of World Investment & Trade 775; Stephan Hobe, Rada Popova, Hussaine El Bajjati and Julian Scheu, 'The Protection of Satellite Telecommunications Activities Under Bilateral Investment Treaties' (2018) 19 Journal of World Investment & Trade 1024; Vivasvat Dadwal and Charles B Rosenberg, 'Looking to the Past for the Future: International Investment Law as a Framework to Protect Private Actors in Outer Space'(2020) 3(3) ITA in review 52; Ingo Baumann, Hussaine El

However, the application of this law to outer space investments is not necessarily straightforward. This is because International Investment Law requires specific conditions for investment protection. Accordingly, and provided that the investment in question qualifies as such within the meaning of the applicable International Investment legal rules, this should be made by a foreign investor in the territory of a certain State, i.e. the host State, and a territorial nexus between the investment and said territory must exist. Seemingly, fulfilling these requirements is rather complex in a scenario, such as that of outer space, where investments and their underlying assets are not always located on Earth but are often located in outer space (i.e. satellites in orbit). In fact, outer space is not subject to "national appropriation by claims of sovereignty"[15] since it constitutes the common "heritage of mankind"[16] and, as such, does not fall under the spatial scope of any International Investment Legal instruments.[17] Therefore, determining the jurisdiction of a certain State with respect to another, and construing the territorial nexus, required under International Investment Law, is rather problematic.

Starting from the above premises, the present work seeks to explore the intersection of these two branches of International Law, namely International Space Law and International Investment Law in the frame of the increasing commercialisation of outer space. More precisely, after determining the scope of application of International Investment Law, it investigates the applicability of the international investment legal framework to private investments made in the context of commercial space activities and, *a fortiori*, the application of Investor State Dispute Settlement, as a dispute settlement mechanism developed within the above body of law, to conflicts between private investors and States arising from the activities carried out in outer space.

Bajjati and Erik Pellander, 'NewSpace: A Wave of Private Investment in Commercial Space Activities and Potential Issues Under International Investment Law' (2018) 19(5-6) Journal of World Investment and Trade 930.

[15] Outer Space Treaty (n 9) at Art. II. At paragraph 1, the Article reads: "*Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means*".

[16] Moon Agreement (n 9) at Article 11. The Article constitutes the hub of the Agreement as under paragraph 1 it states that "*The moon and its natural resources are the common heritage of mankind [...]*", a principle further elaborated under paragraph 5 of the same Article. Notably, it should be noted that the perception of outer space as belonging to humanity as a whole finds general consensus. By way of example, in the Joint Communication to the European Parliament and the Council entitled 'European Union Space Strategy for Security and Defence', the High Representative of the Union for Foreign Affairs and Security Policy explicitly states that 'the EU recognises Outer Space as a Global Common'.

[17] On the interpretation of the principle of 'common heritage of mankind' see, *inter alia*, Seokwoo Lee and Jeong Woo Kim, 'Applying the principle of the common heritage of mankind' in Keyuan Zou (ed), *Global Commons and the Law of the Sea* (Brill Nijhoff 2018) 15-49. Additionally, Rüdiger Wolfrum, 'The Principle of Common Heritage of Mankind' (1983) 43 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 312 and Stephen Gorove, 'The Concept of "Common Heritage of Mankind": A Political, Moral or Legal Innovation?' (1972) 9 San Diego Law Review 390. With regard to outer space specifically, see Virgiliu Pop, 'Is outer space proper the "Common Heritage of Mankind"?' (59th IISL Colloquium on the Law of Outer Space, 2016) 239-246 and Irmgard Marboe, 'The end of the concept of "Common Heritage of Mankind"? The views of state parties to the Moon Agreement' (59th Colloquium on the Law of Outer Space, 2016) 225-238.

2 International Investment Law: the scope of International Investment Protection

Extensively recognised as among the most rapidly evolving branches of International Law, International Investment Law revolves around approximately 3000 International Investment Agreements (IIAs), including 2,340 Bilateral Investment Treaties (BITs) and 319 treaties with investment provisions (TIPs). As mentioned, by encompassing a set of principles, rules, and agreements that guide the relations between foreign investors and their host States, i.e. the States where the investment takes place, International Investment Law is designed to strike a balance between the protection of investors and the regulatory autonomy of the host State.[18] More precisely, International Investment Law aims at encouraging investment flows thus promoting the common interest of the States involved. Accordingly, it seeks to grant investors protection and fair treatment within a structured legal framework, regardless of the location of their investments, at the international level, i.e. beyond and/or outside the domestic jurisdiction of the host State. [19]

Notably, in order to determine the scope of International Investment Law and, *a fortiori*, the extent to which, in case of disputes, investors can resort to Investor-State Dispute Settlement for the protection of their investments,[20] a number of concepts need to be clarified in their essential elements. These are those of foreign investment, investor and the territorial nexus between the investment and the host State.[21]

As concerns the notion of foreign investment, two factors shall be taken into account for the purpose of international investment protection. First, investment is a concept of economic origins which does not find a precise definition under International Law and does not encompass all types of property interests. Second, the relevant investment treaties further define the scope of the investments protected thereinto.[22]

It follows that, while no single definition of foreign investments can be found in the realm of International Investment Law, in practice, international investment legal

[18] Organisation for Economic Co-operation and Development (OECD), 'FDI in Figures. April 2023' (OECD Publishing 2023) <https://www.oecd.org/daf/inv/investment-policy/FDI-in-Figures-April-2023.pdf> accessed 8 March 2024. Despite the drop by 24% in 2022, the global FDI volume reaches an approximate value of USD 1 286 billions.

[19] See Dolzer, Kriebaum and Schreurer (n 13) 20.

[20] In this regard note that, for the purpose of Investor-state Dispute Settlement, international investment agreements have adopted conciliation, meditation and arbitration. In this context, investor-State arbitration has emerged as the dominant method, eclipsing the other two amicable dispute settlement processes. This is not solely due to its adversarial nature, but primarily because it results in binding and enforceable decisions. For further details on Investor-State dispute settlement see, *inter alia*, Dolzer, Kriebaum and Schreurer (n 13) 238. On the emergence of investor-State arbitration over conciliation and mediation see Romesh Weeramantry and Brian Chang, 'Investor-State Conciliation and Mediation', Oxford bibliographies <https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0219.xml> accessed 8 March 2024.

[21] See Barton Legum, 'Defining Investment and Investor: Who is Entitled to Claim?' (2006) 22(4) Arbitration International 521, 522.

[22] Lucy Reed, Zoe Scanlon and Dafina Atanasova, 'Protected Investment', *Max Planck Encyclopedias of International Law* (OUP 2015).

instruments define investment either on an "enterprise" or "asset" basis.[23] According to the former, it is the establishment or the acquisition of an enterprise in the host State that is considered as investment. On the contrary, the latter definition encompasses "every kind of asset", both tangible and intangible, and is normally complemented by an illustrative but non-exhaustive list.[24]

Evidently, the enterprise-based approach entails a higher degree of legal certainty if compared to its counterpart. However, even adopting the asset-based approach, some common traits distinctive to foreign investments can be identified.[25] These include: i) the duration of the project; ii) the regularity of profit and return; iii) the risk for both sides; iv) a substantial commitment; and v) significant impact of the operation for the development of the host State.[26]

On a different note, the definition of investor finds a broader consensus under International Investment Law. While investors can be of two kinds, natural persons and juridical persons, for International Investment Law to apply, specific requirements need to be met which vary depending on the form taken up by the investor. Normally, investors in the form of natural persons are required to be nationals or residents of a State party to the relevant International Investment Agreement or BIT, while investors in the form of juridical persons are to be incorporated or established within a State party to an International Investment Agreement or Bilateral Investment Treaty.[27] In this

[23]See International Institute for Sustainable Development (IISD), 'Definition of Investment' (Sustainability Toolkit for Trade Negotiators) <https://www.iisd.org/toolkits/sustainability-toolkit-for-trade-negotiators/5-investment-provisions/5-2-definition-of-investment/#:~:text=Investment%20can%20be%20defined%20on,enterprise%20in%20the%20host%20state> accessed 6 March 2024. It is noteworthy that, while the asset-based definition is adopted by over ninety percent of investment treaties, the enterprise-based definition is rarely relied upon and can be found, for instance, in Canada bilateral treaty practice.

[24] Dolzer, Kriebaum and Schreurer (n 13) 63. As indicators of the treaty practice with regard to the notion of "asset-based definition of investment", the authors bring three examples. First, the 1991 Argentina-US BIT. Second, the 1992 Ukraine-Denmark BIT, which requires an economic purpose for an asset to qualify as investment. Third, the 2003 USA-Chile BIT which makes reference to the commitment of resources, the expectation of profit and the assumption of risk as necessary characteristics of an investment.

[25] Anastasiya Ugale and Dafina Atanasova, 'Definition of Investment' (*Jus Mundi*, 2023) <https://jusmundi.com/en/document/publication/en-definition-of-investment> accessed 6 March 2024. Although it does not grant legal certainty, this flexible approach entails a number of advantages: not only does it acknowledges the evolving nature of investment but also it accommodates new forms of investment that may emerge over time.

[26] In this regard, Leïla Choukrone and James J Nedumpara, *International Economic Law. Text, Cases and* Materials (CUP 2021). The above listed elements are the elements that the ICSID arbitral tribunal in the Salini case (*Salini Costruttori S.p.A. and Italstrade S.p.A. v. Kingdom of Morocco*, ICSID Case No. ARB/00/4, Decision on Jurisdiction, 23 July 2001 [Salini case]) have indicated when investigating the presence of an investment within the definition provided under the ICSID Convention. Notably, this approach was endorsed by arbitral tribunals in subsequent decisions and is now established in the prevailing jurisprudence.

[27] In this regard note that the Organization for Islamic Cooperation (OIC) constitutes a peculiar type of investor. With its headquarter is Jeddah and 57 member States, The OIC represents and protects the interests of the muslim world. In the context of International Investment Law, the OIC Investment Agreement is worth mentioning since it represents a powerful tool for investment protection inasmuch as it provides protection to foreign investments between OIC Members where no BIT exists. For further details on the matter and on the role played by the OIC as investor see *inter alia* Craig D Gaver and Yusuf Kumtepe, 'Checking in on the OIC Investment Agreement: New Arbitrations, But Slow Progress on Creating A Permanent Dispute Settlement Mechanism' (*Kluwer Arbitration Blog*, 17 March 2023)

regard, it is worth noting that the latter category of investors includes, *inter alia*, private corporations and public entities such as State-Owned Entities (SOEs),[28] Sovereign Wealth Funds (SWFs)[29].

Remarkably, for a foreign investment to enjoy protection under International Investment Law, the fulfilment of the above two requirements alone is not sufficient: a territorial nexus needs to be construed between such investment and the territory of the host State.[30] Leaving aside issues related to the definition of "territory",[31] while determining the existence of this requirement is easily ascertainable for enterprises or tangible assets, it becomes more complex for intangible assets such as contractual rights and financial instruments which do not require a physical transfer of funds into the host State.[32] In such cases, investment tribunals have extended the notion of territoriality requirements as provided for under the relevant international investment legal instrument to encompass situations where the existence of such nexus was less straightforward.[33] By way of example, the fulfilment of the territoriality requirement has been considered achievable through participation via shares or equity in the invested company, even if such participation is remote or indirect.[34] In the same vein, some

<https://arbitrationblog.kluwerarbitration.com/2023/03/17/checking-in-on-the-oic-investment-agreement-new-arbitrations-but-slow-progress-on-creating-a-permanent-dispute-settlement-mechanism/> accessed 6 March 2024.

[28] In this regard, State-owned entities are commonly referred to as entities owned or controlled by States, established with the purpose to achieve financial objectives through a commercial approach. For further details on the matter see Albert Badia and Kabir AN Duggal, 'State-Owned Enterprises' (*Jus mundi*, 2023) <https://jusmundi.com/en/document/publication/en-state-owned-enterprises#:~:text=%E2%80%9CA%20SOE%20%5BState%20Owned%20Enterprise,from%20its%20public%20administrative%20functions.%E2%80%9D> 8 March 2024.

[29] See Xenia Karametaxas, 'Sovereign Wealth Funds as Socially Responsible Investors' in Giovanna Adinolfi, Freya Baetens, Josè Caiado, Angela Lupone and Anna G Micara (eds) *International Economic Law* (Springer 2017). The author defines SWFs as 'public investment vehicles, owned and managed directly or indirectly by governments and set up to achieve a variety of macroeconomic purposes'.

[30] *Inter alia*, Salma Selim and Makane Moïse Mbengue, 'Territoriality of Investment' (*Jus Mundi*, 2023) <https://jusmundi.com/en/document/publication/en-territoriality-of-investment> accessed 6 March 2024. Please, note that numerous International Investment Agreements (IIAs) explicitly mention the territorial aspect of the investment, whereas others remain silent. In this sense, while the latter do not address whether the investment must be made 'within the territory of' the host State, they sometimes make references to the territorial nexus in their Preamble. On the contrary, the ICSID Convention is silent as per whether there should be a territorial link between the investment and the host State to the investment. Nevertheless, the Report of the Executive Directors sets the need to 'stimulate a larger flow of private international investment into the territory of the host State' as the 'primary purpose of the ICSID Convention'. Therefore, with the attempt to fill in the above lacuna, scholars are of the view that the territoriality of the investment is a requirement implicitly enshrined in the body of Article 25 of the Convention.

[31] ibid. In this regard, it should be noted that the issue has turned out to be especially significant in investment disputes concerning State succession and annexation. A recent example is the claims made by Ukrainian investors against Russia regarding investments situated in Crimea which was part of Ukraine before its annexation by Russia in 2014.

[32] ibid.

[33] In this regard see, *Abaclat (formerly Beccara) v. Argentina*, ICSID Case No. ARB/07/5, Decision on Jurisdiction and Admissibility, 4 August 2011 [Abaclat v.Argentina] at paras 374 - 378; 498. Additionally, *Bayview Irrigation District et al. v. United Mexican States*, ICSID Case No. ARB(AF)/05/1, Award, 19 June 2007 [Bayview v. Mexico] at para 98.

[34] Selim and Mbengue (n 30). See also *Teinver S.A., Transportes de Cercanías S.A. and Autobuses Urbanos del Sur S.A. v. Argentina*, ICSID Case No. ARB/09/1, Award, 21 July 2017 [Teinver v. Argentina].

tribunals have suggested that the key factor for determining the location of the investment is whether the host State ultimately benefits from the intangible asset, irrespective of whether direct money transfer into the host State occurred or if foreign forum selection and governing law clauses were established.[35]

3 Investment protection of space assets: the troublesome fulfilment of the territoriality requirement

From the above it is clear that, for an investment to be granted international investment protection under International Investment Law, a number of conditions need to be met. This applies to space assets as well. However, due to the peculiar nature of the outer space scenario and of the space industry as well, such fulfilment is not immediately straightforward. This is first and foremost due to the lack of a generally agreed definition of space assets for the purposes of International Investment Law.[36] In fact, while and as it is the case for the notion of investment under International Investment Law, that of "space assets" is a concept of economic origins not precisely defined under either International Investment Law or International Space Law, the 2012 Space Protocol to the 2001 UNIDROIT Convention on International Interests[37] constitutes the only attempt made by the International Community for the definition of the above term. Despite not pertaining to International Investment Law, under Art. 1 .2 let. (k), the Protocol defines space assets as "any man-made uniquely identifiable asset in space or designed to be launched into space", comprising both moveable and immoveable property potentially located in outer space, including but not limited to satellites. Notably, as it does not encompass certain categories of assets, such as licences or concessions under contract or public law which, especially when relating to the extraction of natural resources, play an important role in the context of space-related investments, such definition can only be regarded as a starting point. In fact, in light of the constant evolution of the space industry, when undertaking an assessment of whether a particular asset qualifies as a space asset, it becomes imperative to depart from considerations strictly pertaining to the legal sphere and, instead, adopt a factual perspective, providing an analysis of the assets that de facto populate outer space/ pertain to the industry although not necessarily located in outer space. In this regard, while the former comprises satellites, space objects, the upper stages of launchers and

[35] Caroline Kleiner and Francesco Costamagna, 'Territoriality in Investment Arbitration: The Case of Financial Instruments' (2018) 9 Journal of International Dispute Settlement 315, 323.
[36] See Cheng (n 8) 462-474.
[37] Protocol to the Convention on International Interests in Mobile Equipment on Matters Specific to Space Assets, 9 March 2012 <https://www.unidroit.org/instruments/security-interests/space-protocol/> accessed 6 March 2024 (not entered into force) [Space Protocol]. Notably, the Protocol under discussion is a Protocol to the Convention on International Interests in Mobile Equipment, 16 November 2001, 2307 UNTS 285 (entered into force on 1 April 2004) [Cape Town Convention].

space stations, the latter includes space mining equipment, private entities engaged in the space sector, contractual rights and, most importantly, concessions contracts for the use of geostationary orbits.

Overall, while based on the above, it can be accepted that space investments in the form of space assets fall under the broad definition of Investment under International Investment Law[38] and are generally made by investors taking up the forms provided by such a body of law, it is the fulfilment of the territoriality requirement to pose particular issues.[39] This is all the more so considering that investments made in the space industry are not necessarily always located on the Earth's surface and within the territory of one State, but are oftentimes located in outer space. Significantly, this makes the ascertainment of the existence of a territorial nexus in the context of investments made in the space sector rather complex.[40] The reason is twofold. First, outer space does not fall under any explicit geographical coverage in the spatial application of a given International Investment Agreement or BIT.[41] Second, as outer space is not subject to claims of national sovereignty,[42] inquiries related to the degree of investment protection granted to space assets in orbits (such as space colonies on Moon or Mars, space transport and space mining activities) by a specific investment treaty arise.[43] It follows that, when it comes to assets in outer space, i.e. in orbit, as it is difficult to determine the territorial limits of the jurisdiction of one State with respect to that of another, it is challenging to establish whether a State can qualify as

[38] As space assets entail a commitment of capital and resources, a certain duration, the expectation of gain or profit and the assumption of risk, they would fall under the definition of investment under the ICSID Convention as well as the generally adopted asset-based/enterprise-based definitions of investment by Bilateral Investment Treaties. See for example, the definition of investment under 2015 India Model BIT at Art. 1(4).

[39]As concerns the challenges related to the construction of a territorial nexus see Luc Colin, 'Washington Arbitration Week 2022: International Investment Protection of Space Assets, Quo Vadis?' (*Kluwer Arbitration Blog*, 28 December 2022) <https://arbitrationblog.kluwerarbitration.com/2022/12/28/washington-arbitration-week-2022-international-investment-protection-of-space-assets-quo-vadis/> accessed 6 March 2024.

[40] Allison Torline, 'Looking Back While Looking Up: A Review of Space Arbitration Topics' (*Kluwer Arbitration Blog*, 22 February 2023) <https://arbitrationblog.kluwerarbitration.com/2023/02/22/looking-back-while-looking-up-a-review-of-space-arbitration-topics/> accessed 6 March 2024.

[41] In this regard note that International Investment Agreements, generally the investment to be made "*in the territory of one contracting party*". Since, from an International Space Law perspective, outer space cannot be subject to national appropriation, investments located in outer space fall outside the geographical coverage of said Agreements. By way of example see Art. 1(4) of the Agreement for the Protection and Promotion of Investment between The Government of the Kyrgyz Republic and the Government of the Republic of Austria, 22 April 2016 <https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5993/download> accessed 6 March 2024 (entered into force on 1 October 2017).

[42] Malanczuk (n 12).

[43] ibid. More precisely, some scholars are of the view that the only factor that matters is whether, from both economic and legal perspectives, the investment, namely the company that possesses assets as property or controls relevant contractual rights, is located within the host State's territory and whether the action affecting the investment, which might potentially constitute a violation of the Bilateral Investment Treaty (BIT), can be attributed to the host State. Therefore, the fact that these assets, i.e. the space assets, would physically be located outside the jurisdiction of the State, would not be of relevance. On the other hand, some other scholars give the utmost importance to the jurisdictional requirement arguing that it is whether the space assets are located under the jurisdiction of the host State that counts.

the host State to the investment and, *a fortiori*, whether possible disputes arising therefrom could be covered by an IIA and solved by means of International Investment Arbitration.

Leaving aside space-related investments on Earth where the territorial nexus has generally been regarded as construed, in the attempt to provide a solution to the complex issue outlined above, a number of approaches have been explored by scholars and adopted by case law. These in principle allow for the establishment of said territorial nexus and, consequently, allow for international investment protection of the abovementioned asset depending on whether they are located in outer space or on Earth.

3.1 Space-related Investments on Earth

As opposed to space investments located in outer space, when it comes to space-related investments on Earth the fulfilment of the territorial requirement does not raise any particular issue.[44]

This category of space-related assets comprises both tangible assets in the territory of a certain State, such as enterprises engaged in the space sector or spacecrafts/rockets before they are launched, and intangible assets – including contractual rights and concession contracts for the use of geostationary orbits. In this case, the ascertainment of the territorial nexus follows the general rules clarified by case law.

Of particular interest is the treatment of intangible assets in the space industry. Against this backdrop, existing case law suggests that the crucial factor in identifying if an investment is located within a particular State is whether that State ultimately benefits from the intangible asset. This holds true irrespective of whether there was a direct financial transfer to the host State or the inclusion of foreign forum selection and governing law clauses.[45] Along these lines, in situations where intangible assets do not require a physical transfer of funds into the host State, the territoriality requirement can be deemed satisfied through share or equity participation in the invested company, even if such participation is remote or indirect.[46] In this context, all three existent

[44] Colin (n 39).
[45] Kleiner and Costamagna (n 35) 323. Among the case law mentioned by the authors, the case of *Abaclat v. Argentina* is of particular relevance. At para 374, the Tribunal ruled: 'The Tribunal finds that the determination of the place of the investment firstly depends on the nature of such investment'. Notably, a settlement agreement between the parties, in the form of an award, closed the case in 2016.
[46] Selim and Mbengue (n 30). Additionally, see *Teinver v. Argentina* (n 34) at paras. 230. In this case, the Tribunal ruled that shares indirectly held through the subsidiaries of a company fell under the coverage of the applicable legal instrument (the 1991 Argentina-Spain BIT). As a matter of fact, the definition of investment provided for by the relevant BIT refers to "every kind of asset", including "property and rights of any kind" thus comprising shares, even in case of indirect or remote participation. For further details on the territorial requirements interpreted in Teinver v. Argentina see Eric De Brabandere, 'Teinver S.A., Transportes de Cercanías S.A. and Autobuses Urbanos del sur S.A. v. The Argentine Republic' (2014) 15 Journal of World Investment and Trade 295, 298.

Investor-State Space cases, namely *CC/Devas v. India*,[47] *Deutsche Telekom v. India*[48] and *Eutelsat v. Mexico*[49] concerned investments belonging to this category.[50] In fact, while the case of *CC/Devas v. India* and that of *Deutsche Telekom v. India* both regarded the lease of a S-band satellite spectrum from Antrix, an Indian State owned entity, to Devas, the case of *Eutelsat v. Mexico* relates to a concession contract granting the rights to the use a geostationary orbital position. Although the cases had inherent differences, it is important to consider that in all three cases the ascertainment of the territorial

[47] *CC/Devas (Mauritius) Ltd., Devas Employees Mauritius Private Limited, and Telcom Devas Mauritius Limited v. Republic of India*, PCA Case No 2013/09 [CC/Devas v. India]. The proceedings, conducted under the 1998 India - Mauritius BIT, arose from the early termination, in 2011, by the Indian Cabinet on Security of the so-called "Devas Agreement" between Devas Multimedia Private Limited, an Indian company with ties to three Mauritian Entities (collectively "CC/Devas") as well as to Deutsche Telekom AG, a German telecommunications conglomerate, and Antrix Corporation Limited, a fully owned Indian Company. The agreement concerned the lease of a portion of S-band satellite spectrum for Antrix to provide multimedia services and broadband wireless access to India remote areas through the Devas System that is a terrestrial-satellite communications infrastructure. Among the claims brought by CC/Devas are the violation of the fair and equitable treatment and the unlawful expropriation of their investments. Notably, the Tribunal ruled in favour of both indirect expropriation and violation of the principle of Fair and Equitable Treatment. For further details on the case and on the ruling of the tribunal see, *inter alia*, Sanjay Sujaya, 'Necessity in Investment Arbitration: Essential Security Interests in the Devas Era' (2021) 3 Indian Arbitration Law Review 15, 18. Additionally, Susannah Moody, 'Mauritius court blocks treaty claim in Devas saga' (*Global Arbitration Review*, 17 January 2023) <https://globalarbitrationreview.com/article/mauritius-court-blocks-treaty-claim-in-devas-saga> accessed 9 March 2024.

[48] *Deutsche Telekom AG v. The Republic of India*, PCA Case No. 2014-10 [Deutsche Telekom v. India]. This case, initiated under the 1995 Germany - India BIT, arises from the same facts leading to the commencement of the arbitral proceedings in CC/Devas vs India, namely the termination of the 'Devas Agreement'. Similarly, to those brought by CC/Devas, the claimants contended the violation of the principle of Fair and Equitable Treatment and that India had unlawfully expropriated their investment. As concerns the outcome of the case, it is worth noting that despite the analogous in the claims and defences, the tribunal found India to have violated the principle of fair and equitable treatment only. On the interpretation of the Fair and Equitable clause in the case of Deutsche Telekom v. India, see Ridhi Kabra, 'Return of the Inconsistent Application of the 'Essential Security Interest' Clause in Investment Treaty Arbitration: CC/Devas v. India and Deutsche Telekom v. India.' (2019) 34(3) ICSID Review - Foreign Investment Law Journal 723, 736-741.

[49] *Eutelsat S.A. v. United Mexican States*, ICSID Case No. ARB(AF)/17/2 [Eutelsat v. Mexico]. Concluded in 2021, it is the most recent publicly known case of investment arbitration arising from space-related activities. Brought before an ICSID Tribunal and administered through the application of the ICSID Arbitration Rules, the case concerns the acquisition by the French company Eutelsat of the Mexican Satellite Company, Satélites Mexicanos ("Satemex") which caters the telecommunication demands of 90 % of the population of the American continent for a value of approximately USD 831 million in 2014. Relevantly, by acquiring the 100 % of the share capital of Satmex, Eutelsat became also the owner of the concessions that were given to said satellite company to occupy geostationary orbital positions in Mexico. Shortly after Eutelsat's investment in Satmex, the government of Mexico implemented regulatory rules requiring satellite operators to allocate a portion of their signal transmission capacity, namely megahertz that could be employed for commercialization, to the use of the government for its own purposes. In this context, deeming to have been obliged to offer a greater amount of megahertz, i.e. 362 megahertz, if compared to its competitors, which instead were required to provide 8 megahertz, Eutelsat commenced the arbitral proceedings. In doing so Eutelsat argued that Mexico had allegedly violated, *inter alia*, the principle of fair and equitable treatment as provided under the 1998 France - Mexico BIT. In 2021, the case was awarded and Eutelsat's claim regarding Mexico's failure to grant fair and equitable treatment was dismissed. The award of the case is not made publicly available. In this regard see Gobierno de México "México prevalece en caso inversionista-Estado promovido por la empresa francesa Eutelsat, S.A. al amparo del APPRI México-Francia" <https://web.archive.org/web/20220309124455/https://www.gob.mx/se/prensa/mexico-prevalece-en-caso-inversionista-estado-promovido-por-la-empresa-francesa-eutelsat-s-a-al-amparo-del-appri-mexico-francia> accessed 9 March 2024.

[50] Colin (n 39).

requirements proceeded relatively smoothly thus demonstrating the non-problematic nature of the territoriality requirement for these types of investments.

3.2 Space Investments in Outer Space: Can a Territorial Nexus be Construed?

As discussed, when it comes to space assets located in outer space, construing a territorial nexus between the investment, i.e. the space asset, and the host State is rather complicated.[51] This is for two reasons, which are largely intertwined with one another. First and foremost, unlike airspace,[52] outer space is not subject to national appropriation by claims of sovereignty.[53] Instead, it constitutes the "common heritage of mankind".[54] Evidently, this results in the determination of - at least physical - boundaries between the different territories in outer space being impossible.

Second, the line of demarcation between airspace, which is subject to the principle of vertical sovereignty, and outer space is far from being agreed upon, thus making it rather controversial to determine when an investment is indeed located in outer space and when, on the contrary, it is located in the airspace.[55] Although this might seem irrelevant for the purposes of our analysis, it instead plays a major role. In fact, in case an investment is deemed to be located in the airspace, the construction of a territorial nexus between the host State and the investment would be rather straightforward as it would follow the same reasoning as the one applied for investments on earth.[56]

Despite the difficulties enshrined in the very peculiar nature of space investments located in outer space, scholars and practitioners have developed several theories in the attempt to - at least tentatively - construe the above territorial nexus and, *a fortiori*, ensure that investments of this kind are granted protection under International Investment Law.

Against this backdrop, before delving into the substance of the subject matter, it is necessary to say a few words on the ruling of the ICSID tribunal in the case of *Abaclat v.*

[51] For the sake of clarity, it should be noted that, for the purposes of our analysis, the category of investments located in outer space encompasses those investments made in the space sector entailing activities carried out in outer space to a large extent.
[52] See the Convention on International Civil Aviation, 7 December 1944, 15 U.N.T.S.295 (entered into force on 4 April 1947). Pursuant to Article I, airspace is governed by the principle of vertical sovereignty, meaning that each state has jurisdiction over the airspace above their territory in accordance with the latin dictum '*cujus est solum, ejus est usque ad coelum*'. More precisely, the Article reads: 'The contracting States recognize that every State has complete and exclusive sovereignty over the airspace above its territory'.
[53] See Outer Space Treaty (n 9) at Art. II.
[54] See Moon Agreement (n 9) at Art. 11.
[55] For further details on the matter see, Colin (n 39). The author points out that while scholars have proposed numerous different limits, an example of which is the Karman line, set at approximately 62 miles above the sea level, even the lowest space objects are orbiting well above this definition.
[56] In this regard see supra section 3.1. Additionally, Jinyuan Su, 'The Delimitation Between Airspace and Outer Space and the Emergence of Aerospace Objects' (2013) 78(2) Journal of Air Law & Commerce 355, 361; additionally, Gbenga Oduntan, 'The Never Ending Dispute: Legal Theories on the Spatial Demarcation Boundary Plane between Airspace and Outer Space' (2003) 1 Hertfordshire Law Journal 64, 64-65.

Argentina, in which the concept of territorial nexus was expanded to extend beyond the physical territory of a State. In this regard, it is noteworthy that, in that case, the investment consisted of the ownership of sovereign bonds issued by Argentina and that the claims were brought forward, following Argentina's default in sovereign bonds resulting from the implementation of laws related to the restructuring of its public debt. Notably, when asked to provide an answer to the jurisdictional issue as to whether the investment in subject was made in the territory of Argentina, the Tribunal ruled that "the determination of the place of the investment firstly depends on the nature of such investment"[57] and that the physical presence is not *per se* fatal to meeting the territorial requirement.[58] In this context, the Tribunal ruled that "the relevant criteria should be where and/or for the benefit of whom the funds are ultimately used, and not the place where the funds were paid out or transferred. Thus, the relevant question is where the invested funds ultimately made available to the host State and did they support the latter's economic development".[59] Therefore, as the funds raised through the bond issuance process were eventually provided to Argentina, contributing to the financing of the country's economic growth, the Tribunal found that the investment was made in the territory of Argentina.[60]

This approach being undisputed and adopted by the majority of the subsequent jurisprudence, it is now time to investigate how the non-physical territorial nexus between a space investment in outer space and the host State can be determined. For this purpose, three different theories will be analysed, the first one of which points towards the registration of the space assets on a certain national registry as a decisive factor to determine whether an investment has been made in the territory of a certain State (3.2.1). On a different note, the second and the third theory under discussion

[57] *Abaclat v.* Argentina (n 33) at para 374. The Tribunal further elaborated on the matter by mandating that, with regard to investments of financial nature, "the relevant criteria should be where and/or for the benefit of whom the funds are ultimately used, and not the place where the funds were paid out or transferred. Thus, the relevant question is where the invested funds ultimately made available to the host State [sic] and did they support the latter's economic development". As reported by Kleiner and Costamagna (n 35) 324, that outlined above is normally referred to by the doctrine as the principle of "continuous credit benefit". In this regard, it is worth noting that in its dissenting opinion, the judge Georges Abi-Saab adopted a different approach. In fact, para 94 reads "And how can the fact that the investment has been made or realised in the territory of the host country be proved or demonstrated, except by tracing it to a specific project, enterprise or activity in that territory that corresponds to the economic meaning of investment in article 25 of the ICSID Convention (i.e. that it contributes to the expansion of the country's productive capacity)".

[58] Notably, this view finds widespread consensus in arbitral investment case law. *Inter alia*, as reported by Hobe, Popova, El Bajjati and Scheu (n 14), see *Ambiente Ufficio SpA and others v. Argentine Republic* ICSID Case No ARB/08/9, Decision on Jurisdiction and Admissibility, 8 February 2013 at para 498. For a critical analysis on the interplay between *Abaclat v. Argentina* and *Ambiente Ufficio SpA*, see Strong S I, 'Heir of Abaclat? Mass and Multiparty Proceedings: Ambiente Ufficio S.P.A. V. Argentine Republic' (2014) 29 ICSID Review-Foreign Investment Law Journal.

[59] *Abaclat v. Argentina* (n 33) at para 376.

[60] *Abaclat v. Argentina,* (n 33) at para 378. For a legal analysis of the ruling see Susan L Karamanian, 'Introductory note to Abaclat & Others v. Argentine Republic: Decision on Jurisdiction and Admissibility (ICSID)' (2013) 52(3) International Legal Materials 667, 667-670.

depart from the above and consider other elements as entailing the potential of establishing said territorial nexus (3.2.2).

3.2.1 Theories Related to Jurisdiction: The Registration of the Space Assets as an Indicator of the Existence of a Territorial Nexus

On the premise that the ICSID Tribunal in *Bayview v. Mexico* has interpreted "investment in the territory of a State" in the sense that the host State should be able to exert jurisdiction over the alleged investment,[61] the first theory under consideration establishes a territorial nexus between the space asset in orbit and the State under whose jurisdiction the asset falls.[62] In this regard, absent any international legal criteria as per the territorial limits of the jurisdiction of a State beyond Earth's atmosphere, one needs to resort to other elements in order to determine the extent to which a certain State has jurisdiction over a space asset when this is located in outer space.

To this end, two International Space Law Treaties come into play: the already mentioned Outer Space Treaty and the Registration Convention. In fact, if read in conjunction, they confer to States the jurisdiction and control over space objects that appear on their national registry.[63] More precisely, as Article VIII of the Outer Space Treaty mandates that States retain jurisdiction over the objects they launch in outer space[64] and Article II of the Registration Convention requires launching States to maintain a registry of said objects,[65] the registration of a space object in a national registry has been considered as an indicator of the existence of a territorial nexus between the investment, i.e. said object, and the host State to the investment, i.e. the State of registry. Accordingly, private investors would in principle be entitled to bring

[61] *Bayview v. Mexico* (n 33), at para 98. On this occasion the ICSID Tribunal ruled that "a salient characteristic will be that the investment is primarily regulated by the law of a State other than the State of the investor's nationality, and that this law is created and applied by that State which is not the State of the investor's nationality". As regulating an investment implies exerting jurisdiction over said investment, the tribunal implicitly considered that of "jurisdiction" as necessary to ascertain the territoriality requirement. Additionally, see the explanatory note of the decision prepared by Shapiro N, 'International Arbitration. *Bayview Irrigation District v.United Mexican States*, ICSID Case No. ARB(AF)/05/1, Award19 June 2007' (2008) 32 Suffolk Transnational Law Review 231.

[62] In this context see Greenwood (n 14) 785. The author specifies that granting investment protection to objects (regardless of whether relating to space or not) within the 'jurisdiction' of a State would align International Investment Law with Human Rights Law which is deeply rooted in this principle.

[63] Hobe, Popova, El Bajjati and Scheu (n 14).

[64] see Outer Space Treaty (n 9) at Art. VIII which reads "A State Party to the Treaty on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object, and over any personnel thereof, while in outer space or on a celestial body. Ownership of objects launched into outer space, including objects landed or constructed on a celestial body, and of their component parts, is not affected by their presence in outer space or on a celestial body or by their return to the Earth. Such objects or component parts found beyond the limits of the State Party to the Treaty on whose registry they are carried shall be returned to that State Party, which shall, upon request, furnish identifying data prior to their return".

[65] See Registration Convention (n 9). Specifically, the Article II reads "When a space object is launched into earth orbit or beyond, the launching State shall register the space object by means of an entry in an appropriate registry which it shall maintain. [...] Where there are two or more launching States in respect of any such space object, they shall jointly determine which one of them shall register the object".

claims before arbitral tribunals against the State in whose national registry the space object they have invested in is registered,[66] as that would be the State exercising jurisdiction over said object.

Significantly, although pertaining to another sphere of international law, the Space Protocol to the Cape Town Convention can be relied upon in support of this approach. In fact, the Space Protocol stipulates that, for the purposes of an "international transaction" within the meaning of the Convention, a space asset must be physically located in the territory of the State of Registry.[67] Despite not straightforward, this might be interpreted as demonstrating how, in the eyes of the International Community, a territorial link between the State of registry and the space assets exists and, consequently, that the requirement of registration of a space asset may serve as an indicator of its international, and *a fortiori,* foreign dimension as an investment.

It is important to note, however, that this theory does not find general consensus. In fact, there are slightly opposite perspectives arguing that whether space assets fall under the jurisdiction of the host State may not be the decisive factor for the purposes of the territoriality requirement.[68] Conversely, what would hold greater significance is whether, from both economic and legal standpoints, the investment is situated within the host State's territory and whether the action that disrupts the investment can be attributed to the host State.[69]

3.2.2 Possibly Relevant Factors Beyond the Registration of the Space Assets

As mentioned, factors other than the registration of a space asset have been interpreted as establishing a territorial link between said asset and its host State. Notably, as they are not *per se* indicative of the investment being made in the territory of a certain State, such factors form the basis of theories that depart from the concept for which the investment must occur within the territory of a State for the purposes of construing the territorial nexus and, instead, opt for a broader interpretation.

In this context, the first theory under analysis applies to the case of a damage to a space asset occurring in outer space. Accordingly, when a State in the exercise of its

[66] As reported by Colin L, 'Washington Arbitration Week 2022: International Investment Protection of Space Assets, Quo Vadis?' supra note 39, it should be noted that the adoption of this approach could, in principle, result in a contentious scenario where, respondent States, when brought before an arbitral tribunal in relation to an investment in outer space, could possibly deny the existence of a territorial nexus between their territory and said investment. On the contrary, investors would be prone to support a broader interpretation of the notion of "territory of the investor" including, thereinto, any territory over which the State retains jurisdiction and control.

[67] In this regard see Baumann, El Bajjati and Pellander (n 14) 930. Additionally, Hobe, Popova, El Bajjati and Scheu (n 14).

[68] Malanczuk (n 12).

[69] ibid.

activities causes such a damage and when this damage has a negative impact on Earth, a territorial link may be constructed between the State and the space asset in question.[70]

An example of the application of this theory is the hypothetical collision between space debris stemming from a government-owned satellite irresponsibly managed by State A and the spacecraft of a space tourism company incorporated in State A. Provided that such damage is caused by the improper conduct of State A, if this has negative consequences on Earth, resulting, for example, in a reduction of the value of the shares owned by a foreign investor established in State B who has invested in the space tourism company and, *a fortiori,* in the spacecraft, it is possible to imagine a territorial nexus between the investment and the State A. It follows that the foreign investor would be entitled to bring a claim against such State on the basis of the BIT concluded between State B (i.e., the home State to the investor) and State A (i.e., the host State to the investment), if any.[71] This is not because the investment would be made in State A but, instead, because the obligation of State A to protect the investment would encompass the outer space activities undertaken by objects under its jurisdiction.

On a slightly different note, the second approach under discussion which also departs from considerations related *stricto sensu* to the concept of jurisdiction, applies to the specific case of the licence of usage rights for orbital slots and frequency bands. In this situation, a territorial link may be established with the State that issues the licence on the basis of a licence agreement and upon the payment of licence fees. One may reach this conclusion on a twofold basis: first, the already mentioned judgement in *Abaclat v. Argentina*, which mandates to examine the presence of a territorial nexus depending on the nature of the investment; second, the existing arbitral practice with regard to financial instruments that, for the purposes of the construction of the territorial nexus, focuses not on the location of the funds but on the State actually benefiting from them.[72] It follows that, since the issuing State directly benefits from the payments under the licence agreement, the territorial requirement may be regarded as met, provided

[70] For further details on this matter see, Colin (n 39).

[71] Note that slightly different is the case of Kosmos 954, a satellite launched in orbit by the Soviet Union in 1977. Due to a malfunction, when the satellite re-entered orbit the following year, it dispersed radioactive fragments across northern Canada, thus causing damage within the Canadian borders. On that occasion, as two States were involved, Canada brought claims against the Soviet Union for the compensation of damages on the basis of the 1972 Liability Convention read in conjunction with the 1975 Registration Convention.

[72] In this regard see, *Ambiente Ufficio S.p.A. and others v. Argentine Republic* (n 58). At para 499 the Tribunal ruled: "[...] in order to identify in which State's territory an investment was made, one has to determine first which State benefits from this investment. Most observers will agree that the one criterion which may be taken from the ICSID Convention itself when it comes to determining the nature of an investment under this Convention, is that of a contribution "for economic development", as referred to in the first preambular paragraph of the ICSID Convention. Accordingly, to assess where an investment was made, the criterion must be to whose economic development an investment contributed". For the further analysis of the ruling of the case see, *inter alia,* the explanatory note of Sadie Blanchard, 'Ambiente Ufficio S.p.A. and Others v. Argentine Republic' (2014) 15(1-2) Journal of World Investment & Trade 314.

that the State issuing the licence is other than the State of nationality of the private investor acquiring it.[73]

From a practical perspective and still remaining in the frame of space debris collisions, this theory, related to the licence of usage rights for orbital slots and frequency bands, could find application in case of a crash between space debris originating from the non-disposal of a government-owned spacecraft by State A and a satellite owned by a company established in State B but using frequency bands granted by State A by means of a licence agreement and upon payment of a licence fee. In this scenario, a territorial nexus could be construed with the State issuing the licence. Therefore, the company affected by the collision (i.e., the private investor) could in principle bring a claim against State A as long as an International Investment Treaty, whether of multilateral or bilateral nature, between State A and State B is in place.[74] Notably, this scenario, although hypothetical, is increasingly likely to occur. In fact, while there is a growing number of satellites and space objects orbiting in outer space, not enough satellites are being removed at the end of their life span. This could lead to an increase in the number of "in space collisions" and, due to the overcrowding of the Low-Earth Orbit (LEO) to a high risk of a "Kessler effect" with a single collision setting off a chain reaction of additional collisions.[75]

4 Conclusions: The Possible Role of Investor-State Dispute Settlement in Outer Space Activities

As outlined in the preceding paragraphs, at the state of play and as opposed to International Space Law, International Investment Law is capable of establishing a structured legal framework for private investment in outer space.

In fact, it has been demonstrated that space-related investments of private or commercial nature, can enjoy protection under International Investment Law as the requirements posed therein can in principle be fulfilled. Notably, this holds true not only in the case of investments located on the Earth's surface, but arguably also in the more complex scenario of investments located in outer space.

In regard of the latter, while space-related investments, whether on Earth or in outer space, fit the definition of investment under the relevant International Investment legal instruments without any apparent difficulty, for the purposes of including them within the scope of international investment legal sources the establishment of the territorial

[73] Malanczuk (n 12) 971.
[74] See Colin (n 39).
[75] See Scott Atkins and Andrew Battisson, 'Dispute Resolution and Restructuring in Outer Space: Using ADR to Drive Efficiency and Better Outcomes for Creditors' (Norton Rose Fulbright Publications, 2022) <https://www.nortonrosefulbright.com/en/knowledge/publications/5bf5d3bb/dispute-resolution-and-restructuring-in-outer-space> accessed 9 March 2024.

nexus between the investment and the host State can be a complex matter. This is particularly apparent when it comes to space-related investment in outer space. In fact, although the inherent characteristics of outer space as a *locus* not subject to national appropriation and, therefore, devoid of interstate borders and outside any domestic jurisdiction would seem to suggest that such a link cannot be constructed, theories have been developed that point in the opposite direction.[76] At present, they are relatively limited in number and primarily fall into two categories: on the one hand, theories that identify the registration of the space object in a national registry as the indicator of the existence of a territorial nexus between that object and the State of registry; on the other hand theories that, instead, rely on other factors such as the possible negative impact on Earth of a damage to a space asset occurring in outer space or the benefits deriving from a concession or licence agreement to a certain State. However, despite their innovative nature, both these categories are not without drawbacks, particularly in relation to their limited applicability. While the former, consisting of the theories related to the registration of the space asset, applies only provided that such registration has been carried out, the application of the latter, is even more circumscribed as it is subject of the co-existence of a number of different factors which are either highly specific, i.e. the occurrence of a damage in outer space with a negative impact on Earth, or difficult to ascertain, i.e. determining the end-receiver of the benefits deriving from a licence or concession contract.

Nevertheless, since the matter has come to the attention of doctrine only recently, concurrently with the development of the space industry and commercialization of space, it is expected that new theories will be developed in the near future.

Insofar as space-related investments can be granted investment protection under International Investment Law, it follows that Investor-State disputes arising in relation to such investments can be resolved by means of Investor-State Dispute Settlement. This is very interesting for investors, in the absence of any precise dispute resolution mechanisms available to them under International Space Law.

Against this backdrop, the exact role that Investor-State Dispute Settlement would play in the frame of Investor-State disputes arising in outer space from commercial space activities, such as those resulting from outer space collisions involving space-related investments, is not clear yet. The reason lies in the lack of precedents, with the few Investor-State space cases up to date only concerning disputes that, although involving space-related investments, arose on Earth.[77]

[76] In this regard, as already mentioned, see Outer Space Treaty (n 17) at Art II. Notably, the theories that have been developed identify the spatial nexus by going beyond the spatial dimension and referring to a number of other factors including the registration of the space object, when this constitutes the investment.

[77] It is noteworthy that all three existing Investor-State Space Case Law revolve around disputes arising on Earth in relation to space-related investments. More precisely, in the Devas Saga, the element giving rise to the arbitration proceedings was the termination of the so-called Devas Agreement, a contract for the construction, launch and

In any case, envisaging the applicability of Investor-State Dispute Settlement to outer space disputes looks reasonable. This is not only because the requirements for triggering the international investment protection of space-related investments located in outer space can be met, which is a sufficient reason in itself, but also because investors investing in outer space face similar challenges as the ones investing on Earth. In fact, and despite the unique challenges and risks that outer space investments pose, these challenges include questions of fair and equitable treatment and expropriation, which are the standards most commonly involved in Investor-State disputes.[78] Evidently, these similarities support the application of Investor-State Dispute Settlement in a way akin to terrestrial disputes.

Furthermore, it is the *rationale* behind International Investment protection that justifies the extension of Investor-State Dispute Settlement to encompass outer space disputes. In fact, such extension would be in line with the fundamental purpose of Investor-State Dispute Settlement which, by providing a mechanism for addressing disputes, seeks to provide investors with international investment protection and fair treatment irrespective of where their investments are located.[79]

From a slightly different perspective, provided that Investor-State Dispute Settlement aims, *inter alia*, at encouraging investment flows and promoting the common interest of the States involved, both these objectives would be met by turning the latter in the default dispute settlement mechanisms for conflicts between private investors and States, arising in outer space from commercial space activities.

In fact, enhanced legal certainty and predictability as per the mechanisms available for the settlement of outer space disputes have the potential to encourage investments in the space industry given that investors are more likely to invest when they have an understanding of the way the potentially arising disputes could be resolved.[80] Additionally, taking a related but somewhat different angle, it is noteworthy that the

operation of two satellites and the lease of satellite transponder capacity. On a slightly different note, the case of Eutelsat v. Mexico concerned the lease of geostationary orbits.

[78] Sebastian King, 'Incentivising Commercial Space Activities through International Investment Arbitration' (*Kluwer Arbitration Blog*, 31 October 2020) <https://arbitrationblog.kluwerarbitration.com/2020/10/31/incentivising-commercial-space-activities-through-international-investment-arbitration/> accessed 8 March 2024. Additionally, Dolzer, Kriebaum and Schreurer (n 13) 130. For the sake of comprehensiveness, it is noteworthy that under International Investment Law, the principle of Fair and Equitable Treatments concerns the treatment to be accorded to the foreign investor in the host State. Slightly differently, that of protection from expropriation is a principle of customary origins which requires a state to pay compensation when it expropriates the property of a foreign investor.

[79] On the rationale of ISDS see Dolzer, Kriebaum and Schreurer (n 13) at 20. Additionally, Choi Won-Mog, 'The Present and Future of the Investor-State Dispute Settlement Paradigm' (2007) 10 Journal of International Economic Law 725, 740. However, as is well known, ISDS has been the centre of a legitimacy crisis mostly due to the consistency and predictability of arbitral decisions, the lack of transparency and the fragmentation of the applicable legal instruments. For an overview of the criticisms underlying ISDS, see, among many others, Chen Yu, *Dispute Settlement and the Reform of International Investment Law* (Edward Elgar Publishing 2023).

[80] Atkins and Battisson (n 75). Additionally, Hanneke L van Traa-Engelman, 'Legal Requirements Constituting a Basic Incentive for Private Enterprise Involvement in the Commercialization of Space Activities' (1995) 38 Proceedings on the Law of Outer Space 3.

application of Investor-State Dispute Settlement has been regarded as a possible contribution to mitigate the creation of space debris. This is because, absent any international treaty laying down a precise framework to prevent the creation of space debris, the application of Investor-State Dispute Settlement might serve as a mechanism that, by imposing liability risks, encourages States to strengthen their national measures directed at avoiding the formation of space debris.[81] As the latter poses significant hazards to active spacecrafts and the long term sustainability of commercial space activities, mitigating space debris would not only ensure the safety of assets in space but also help maintain the overall accessibility of outer space for the international community, thus promoting the common interest.[82]

From the above, the potential of Investor-State Dispute Settlement in the frame of disputes arising in outer space from commercial space activities is noteworthy. However, it remains to be seen how (and if) this potential will be fully implemented. In this sense, the wait will most likely not be long: the increasing commercialisation of outer space will lead to more and more disputes between States and investors which will in turn test the boundaries of Investor-State Dispute Settlement and its effectiveness to solve these disputes arising in the frame of such a rapidly evolving context.

[81] In this regard see, Laura Yvonne Zielinski, 'Space Arbitration: Could Investor-State Dispute Settlement Help Mitigate the Creation of Space Debris?' (*EJIL:Talk!*, 19 March 2021) <https://www.ejiltalk.org/space-arbitration-could-investor-state-dispute-settlement-help-mitigate-the-creation-of-space-debris/> accessed: 8 March 2024.

[82] For an overview of the risks posed by space debris see European Space Agency (ESA) 'ESA's Annual Space Environment Report' (ESA Publishing Office, 12 September 2023). The Report shows that the most severe threat posed by orbital debris is the potential occurrence of a Kessler Syndrome event, where an in-space collision triggers a cascading chain reaction, rendering low Earth orbit (LEO) inaccessible and spaceflight hazardous to undertake for many generations to come. Additionally, European Space Agency (ESA) 'Space Debris: Assessing the Risk' (*ESA.int*, 21 March 2005) <https://www.esa.int/Enabling_Support/Operations/Space_debris_assessing_the_risk> accessed 8 March 2024; J Armand Musey, 'Op-ed | Orbital debris and the threat to industry investment' (Spacenews, 1 November 2020) <https://spacenews.com/op-ed-orbital-debris-and-the-threat-to-industry-investment/> accessed 8 March 2024.

*Giovanni Tricco**

THE NEW TRANSATLANTIC DATA AGREEMENT PLACED IN CONTEXT: DECODING THE SCHREMS SAGA WITHIN THE DIGITAL ECONOMY

Abstract

Any time we use digital services we create data. That data travels around continents, constituting the fundamentals of the digital economy. Begun in 2015, the Agreements that allowed this kind of free flow of data between the EU and the US have been invalidated – the Safe Harbour and the Privacy Shield – bringing uncertainty in the work of over 5300 companies that based their practices on such frameworks which allowed data to move borderless, as well as, threatening the digital rights of European citizens who do not see their data adequately protected across the Atlantic. Indeed, in Data Protection Commission v. Facebook Ireland – Schrems II – the CJEU claimed that US surveillance law offers inadequate safeguards for EU citizens' data. In the summer of 2023, the transatlantic actor unlocked the gridlock with the new adequacy decision of the EU based on the new Transatlantic Data Privacy Framework, amid debate on the adequacy offered by it. The question of whether the new pact will ensure long-standing data flow between the two sides of the Atlantic remains open.

The question is of extreme importance, such data transfers are fundamental to conducting international trade and commerce in today's globally connected world. Therefore, people and businesses can use cross-border data flows to communicate online, map global supply chains, share research, provide cross-border services, and drive technological innovation. The trade and investment relationships between the US and the EU are broad and highly intertwined. The United States and the European Union have the highest cross-border data flows in the world, valued at $7.1 trillion dollars annually, which are critical to much of the economic interaction between the two countries. The article aims to shed light on the problems experienced with the invalidation of the previous two agreements, with an analysis of American surveillance laws and questioning whether the new agreement could be the base for a stable transatlantic digital economy.

JEL CLASSIFICATION: F52; K24; K33; L38.

SUMMARY

* PhD candidate in the Joint International Doctorate in Law, Science and Technology at the University of Bologna & Vrije Universiteit Brussel.

surveillance law – 3.1 Case-law as basis for the wide scope of U.S. foreigner surveillance law – 3.2 United States foreign surveillance law: section 702 FISA and Executive Order 12333 – 3.2.1 The Foreign Intelligence Surveillance Act (FISA): section 702 – 3.2.2 Executive Order 12333 and PPD-28 – 4 Towards a stable digital economy or unfolding a new chapter in the Schrems saga? – 5 Conclusions

1 Introduction

On the 10th of July 2023, the European Union granted an adequacy decision based on the new Transatlantic Data Privacy Framework to heal the gridlock that the digital economy was facing. The research intends to navigate the challenges that the new Privacy Framework will face in the time ahead to pass the test of a well-expected Schrems III. Namely posing appropriate safeguards against the intrusion of US surveillance authorities in European data and the establishment of a functional court to ensure judicial redress for Europeans in case of misuse of their data.

The two transatlantic actors adopted historically different approaches to privacy and the protection of data. The EU considers the privacy of communications and the protection of personal data as fundamental rights, under EU law, whilst US law protects certain data on a sectoral basis, without comprehensive federal legislation. These differing approaches have resulted in a discernible privacy law gap. The research accompanies the readers on the differences and similarities between the two frameworks and surveillance capabilities, till analysing the possible legal and policy challenges that must be overcome to ensure that the new Framework will withstand a new challenge in the European courts.

The article will be structured in three main sections. The first section aims to describe and explore the scenario surrounding EU-US Data transfer agreements, from an economic, legal, and political perspective. Thus, it continues with a brief analysis of European Data Protection Law and compares the different approaches to privacy and data protection on the two sides of the Atlantic. Indeed, the disagreement between the transatlantic actors is a consequence of different approaches, understanding, and cultures of privacy and data protection, each with its intuitive sensibility that has resulted in two very diverse privacy laws. An analysis of the development of privacy law on both sides of the Atlantic is needed to understand the actual situation. Then, it concludes with an analysis of the failure of the two previous data transfer agreements.

The second section explores the main reason for the concerns of the CJEU, namely United States Surveillance law, through an analysis of the case law that has widened the capabilities of the U.S. Intelligence Communities over the years, as well as the laws that confer such powers to the U.S. authorities: section 702 of the Foreign Intelligence Service Act and Executive Order 12333.

The third section tries to analyse whether the new Privacy framework negotiated by European and United States officials will satisfy the concerns raised by the CJEU in

Schrems II, to constitute a proper and stable new 'Enhanced Privacy Shield' that would constitute a stable basement for the digital economy.

The topic is of extreme importance, first to ensure an adequate level of protection of citizens' data, secondly to foster the interoperability and openness of the internet to permit the digital economy to flourish as a borderless data economy in the near future of safe digital trade.

2 Transatlantic Data Transfers Placed In Context: Political, Historical, And Economical Considerations

The stakes are high, in the near future if a transatlantic data agreement does not survive the scrutiny of the CJEU legal uncertainty will persist and future economic losses for the digital economy of the EU and the U.S. will escalate. According to forecasts of DIGITALEUROPE by 2030 if a stable agreement that enables lawful and consistent data transfer is not in place the European Union economy could lose:

- €1.3 trillion in cumulative economic growth by 2030, which is the equivalent of the GDP of the Spanish economy each year.
- €116 billion in annual exports, which is the equivalent of the annual exports of Sweden or the aggregate annual export of several smaller Members of the EU.
- 1.3 million job losses, primarily high-skilled professions.

If the agreement constitutes a stable mechanism of data transfer the EU economy would benefit from:

- €720 billion in cumulative extra growth by 2030, equivalent to an increase of 0.6% in GDP every year.
- €60 billion in annual exports, of which half come from the manufacturing sector, boosting the position of European SMEs.
- 700 thousand new jobs will be created.[1]

Hence, it is crucial that the new agreement constitute a lasting Data Flow agreement, fostering, and sustaining the data economy. The article questions whether this will be the case or if another Schrems saga looms on the horizon.

[1] DIGITALEUROPE, 'Data Flows & the Digital Decade' (2021) <https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/DIGITALEUROPE_Data-flows-and-the-Digital-Decade.pdf> accessed 11 March 2024. Digital Europe is a trade association representing the interest of the tech industry in Europe.

2.1 A different approach on privacy and data protection

The disagreement between the transatlantic actors resulted from a different approach, understanding, and cultural background of privacy and data protection, each with its intuitive sensibility that has resulted in two diverse privacy laws.[2] An analysis of the development of privacy law on both sides of the Atlantic is needed to understand the diatribes experienced.

Notwithstanding, in both Europe and the United States, early discussions regarding data protection and privacy focused on the same concern about increasing surveillance capabilities of government and administrative bodies.[3] Nevertheless, a consensus arose that the 'fair information principles'[4], which define how personal information should be handled, would be the best way to address these concerns. These principles centred on policies of transparency on the use, disclosure, secondary use, correction, and security of personal data. However, the principles did not lay out specific legal obligations, although they did give a framework for weighing data privacy against other considerations.[5] Therefore, since their establishment, the fair information principles guided the United States approach regarding privacy protection.[6] Moreover, their influence extended far beyond the United States, the ideas provided the groundwork for the adoption of future legal frameworks worldwide. Indeed, not just for U.S. laws such as the Privacy Act of 1974[7], but also for the first data protection laws implemented in Western Europe such as in France and Germany in the 1970s.[8] For example, the Lander of Hesse in Germany established the first data protection law worldwide in 1970.[9] The latter was followed by Germany and France which adopted the first federal and national data protection legislation in 1978.[10]

Although the principles adopted by Western democracies in the early 1970s were similar, significant disparities soon appeared in how such policies should be implemented and who would fall within their scope. The initial discussion focused on

[2] James Q Whitman, 'The two western cultures of privacy: Dignity versus liberty' (2003) 113 Yale LJ 1151.
[3] Colin J Bennett '*Regulating privacy*' (Cornell University Press 2018).
[4] IAPP, 'Fair Information Practice Principle' <https://iapp.org/resources/article/fair-information-practices/> accessed 11 March 2024.
[5] Robert Gellman, 'Fair Information Practices: A Basic History' Version 2.22 (2022) <file:///C:/Users/tmikoni/Downloads/SSRN-id2415020.pdf> accessed 11 March 2024.
[6] Alan F Westin, 'Social and political dimensions of privacy (2003) 59(2) Journal of social issues 431.
[7] The United States Department of Justice, 'The Privacy Act of 1974' <https://www.justice.gov/opcl/privacy-act-1974> accessed 11 March 2024.
[8] Marc Rotenberg, 'Fair information practices and the architecture of privacy (What Larry doesn't get)' [2001] Stanford Technology Law Review 1.
[9] Government of the state of Hessel, 'Data Protection Act 1970' <https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes> accessed 11 March 2024.
[10] For France, see Loi N° 78-17, 6 January 1978 <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460?init=true&page=1&query=Loi+N%C2%B0+78-17&searchField=ALL&tab_selection=all> accessed 11 March 2024; for Germany, Federal Data Protection Act 1977 <https://www.gesetze-im-internet.de/englisch_bdsg> accessed 11 March 2024.

discussion on governmental use of personal data quickly evolved to encompass the private industry as more private enterprises advanced their data processing methods to gather considerable amounts of personal data for business goals, therefore, advocating the government to adopt business-friendly laws.[11]

Disagreements on how to construct such legal frameworks and policies result from different values and cultures on which different legal systems are based as stated by Whitman: "*any person has legal and social values of the societies in which we live. In particular, we have […] intuitions that reflect our knowledge of, and commitment to, the basic legal values of our culture.*"[12] Therefore, as a result, different approaches take place. Such variances can be connected to the conceptions of privacy designed by Post namely: "*privacy as an aspect of dignity and privacy as an aspect of liberty.*"[13] The European approach to privacy is based on the concept of dignity, while the American approach is based on the pursuit of liberty. The former is concerned with the right to govern the information that is made public about oneself to maintain control over one's public image; the latter is much more focused on liberty versus the state, i.e., freedom against government intrusion.[14]

In addition, the past history of fascist and totalitarian governments in Europe affected many European countries' perspectives on data privacy adding to the European political class and citizens' requests for rigorous data protection procedures, particularly for personal data, for example, Nazis through the control of the state and information technology were able to continuously abuse private data to detect Jews or other minority groups.[15] Consequently, Germany was one of the initial nations to implement data privacy regulations as a result of Nazism atrocity and World War II, Germans remain particularly worried about invasions of privacy even on these days.[16]

It is acknowledged that both the transatlantic actors are devoted to protecting individual privacy rights and personal data. Nonetheless, the approaches in the United States and the European Union can result in nuanced differences. Therefore, variances in values and approaches are reflected in the difficulties that the international community has faced.

[11] Monika Zalnieriute, 'Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National Security' (2022) 55(1) Vanderbilt Journal of Transnational Law 1.
[12] James Q Whitman (n 2) 1160.
[13] Robert C Post, 'Three concepts of privacy' (2001) 89 Geo LJ 2087.
[14] James Q Whitman (n 2).
[15] Olivia B Waxman, 'The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History' (*Time*, 24 May 2018) <https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/> accessed 11 March 2024.
[16] James B Rule and Graham W Greenleaf, *Global privacy protection: the first generation* (Edward Elgar Publishing 2010).

2.2 The European approach

The EU considers privacy and personal data protection to be fundamental rights. Indeed, these rights are included in Article 7 and Article 8 of the European Union's Charter of Fundamental Rights (CFREU)[17], which has binding force on all EU member states by its adoption as primary law in the Treaty of Lisbon in 2009. These rights granted by the Charter, which are comparable to a constitutional right in the United States[18], are based on Art.8 of the European Convention of Human Rights (ECHR).[19] Furthermore, Article 52 of the CFREU states that any restrictions on such rights must adhere to the proportionality principle, while Article 47 guarantees to every European citizen the right to seek judicial redress for any violations.[20] Thus, all the jurisdictions to which the data of European citizens are addressed cannot circumvent those principles that are integral parts of EU law, it must be ensured the protection of personal data, their process according to the principle of proportionality, and a mechanism of redress must be assured for any case of disuse of data. For Europe, the protection of privacy and data protection has always been at the centre of the political agenda since the adoption of the Data Protection Directive and then to the adoption of the General Data Protection Regulation in 2018. As already mentioned, the GDPR created a set of standards directly enforceable and consistent for personal data protection across the EU aiming to protect people's fundamental rights in the digital era. Moreover, Chapter V GDPR linked to the principles enshrined in the CFREU covers the outward dimension of data to guarantee the same level of protection for European data outside the EU.

2.3 The United States approach

Unlike the EU, in the United States there is no federal legislation that controls the acquisition and use of personal data of consumers. However, The U.S. Supreme Court has inferred from the Constitution an individual's right to privacy, with a mainly focus on the protection from government interference, indeed the 4th Amendment encompasses the "search and seizure" provisions which provide that: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"[21] The Amendment derives from

[17] Charter of Fundamental Rights of the European Union 2012/C 326/02 of 26 October 2012 [2012] OJ C326/391.
[18] Emily Linn, 'A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-US Privacy Shield Agreement' (2017) 50 Vanderbilt Journal of Transnational Law 1311.
[19] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11 and 14).
[20] Kristin Archick and Rachel F Fefer, 'U.S. – EU Privacy Shield and Transatlantic Data Flows' (2021) Congressional Research Service <https://crsreports.congress.gov/product/pdf/R/R46917> accessed 11 March 2024.
[21] U.S. Constitution., IV amendment.

the notion that each man's home is his castle and that such a 'castle' shall not be violated by any government interference.[22] In addition, in *Katz v. United States*[23] has been acknowledged that the Amendment "protects people, not places," eliminating the requirement of real physical trespass and subjecting electronic surveillance to the Amendment's restrictions, furthermore it was established the so-called expectation of privacy test upon which one may 'justifiably' rely to preserve as private what expected to maintain as such, even in public from the interference of the authorities.[24]

Moreover, the leeway of the federal government has been restricted by The Privacy Act of 1974 which regulates how the federal government handles personal information to guarantee that data held by federal agencies are not disclosed without consent, except for certain exemptions[25], on the other hand, the Electronic Communications Privacy Act of 1986 placed upon governmental officials' restrictions on telephone wiretaps such as electronic data transmission.[26]

Furthermore, since the limitation in the constitution to protect the data of citizens and the lack of a unique federal law that governs data protection several federal laws have been adopted by Congress to give statutory protections for citizens' personal information.[27] Indeed, rather than a single complete comprehensive regulation, the United States adopted in the years a kind of 'patchwork' of federal laws that regulate firms' data protection practices.[28] The United States adopted a specific sectoral approach, trusting on a mixture of legislation, regulation, and self-regulation. These laws vary in scope depending on who is in charge of enforcement and the kind of penalty related to them. Among these laws actually in force in the U.S. are: Children's Online Privacy Protection Act (COPPA); Electronic Communications Privacy Act (ECPA); Health Insurance Portability and Accountability Act (HIPAA); Federal Trade Commission Act (FTC Act) et. all.[29]

Therefore, the type and grade of protection granted to data depends on which sectors the data are processed and which federal law covers that circumstance. As an example, *The U.S. laws protect specialized information, such as health care or financial data, by implementing a data-specific approach to regulating data privacy. In these cases, The*

[22] Cornell Law School, Fourth Amendment, Legal Information Institute, <https://www.law.cornell.edu/constitution/fourth_amendment> accessed 11 March 2024.
[23] *Katz v. United States* 389 U.S. 347 (1967).
[24] Cornell Law School, 'Katz and the Adoption of the Reasonable Expectation of Privacy Test' Legal Information Institute <https://www.law.cornell.edu/constitution-conan/amendment-4/katz-and-the-adoption-of-the-reasonable-expectation-of-privacy-test> accessed 11 March 2024.
[25] The Privacy Act of 1974 (n 7).
[26] Electronic Communications Privacy Act of 1986 <https://www.congress.gov/bill> accessed 11 March 2024.
[27] Stephen P Mulligan and Chris D Linebaugh, 'Data Protection and Privacy Law: An Introduction' (2019) Congressional Research Service <https://crsreports.congress.gov/product/pdf/IF/IF11207> accessed 11 March 2024.
[28] Zachary S Heck, 'A Litigator's Primer on European Union and American Privacy Laws and Regulations' (2018) 44 Litigation 59.
[29] For the full list see note 27.

Federal Trade Commission (FTC) has the authority to pursue enforcement proceedings against corporations that mislead customers about their privacy practices, however, it lacks the authority to enforce comprehensive online privacy standards.[30] On the other hand, other laws apply comparable principles to private businesses. The Stored Communications Act (SCA) which is part of the ECPA, bans internet service providers from unlawfully accessing or disclosing some electronic communications.[31] Moreover, several laws while just not limited to data protection, impose restrictions on the businesses' procedure to manage personal information. As an example, The FTC Act bans misleading procedures that could be carried out by companies.[32]

From the point of view of general regulation for private entities and their practices, it is well-established self-regulation through industry best practices.[33] Indeed, the typical U.S. liberal approach has fostered the self-regulatory regime in order to foster innovation in fast-paced sectors such as artificial intelligence (AI) or e-commerce that base their functioning on the process of consumer data. Such an approach gives businesses the possibility to adapt easily to shifts in technological innovation while assuring a better business-oriented framework, therefore instead of relying on government authority for enforcement, the U.S. model relies on self-policing. Notwithstanding, a part of the public opinion advocates for stronger laws on privacy in the U.S. supporting the view that gaps are present in the actual legal framework.[34]

In conclusion, while the EU views privacy protection as a fundamental human right, the United States views these rights as a commodity, leaving the matter to market forces.[35] The United States employs a risk-based approach in which companies are legally responsible for managing data wherever it is transferred and stored, in opposition we have seen that the EU takes a more rigid compliance-based approach since data is considered embedded in every person, then needing fundamental protection.[36] Therefore, it is understandable that the difficulties in concluding a stable agreement for international transfer result from nuanced differences in histories, cultures, and values between the two transatlantic actors.

[30] Archick and Fefer (n 20).
[31] Charles Doyle, 'Privacy: An Overview of the Electronic Communications Privacy Act' (2012) Congressional Research Service <https://crsreports.congress.gov/product/pdf/R/R41733> accessed 22 March 2024.
[32] Federal Trade Commission Act (1914) 15 U.S.C. §§ 41-58.
[33] Sandeep Mittal, 'Critical Analysis of Divergent Approaches to Protection of Personal Data' (2017) 8(7) International Journal of Advanced Research in Computer Science 58.
[34] Archick and Fefer (n 20).
[35] Stephen J Kobrin, 'Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance' (2004) 30(1) Review of International Studies 111.
[36] Nigel Cory, Daniel Castro and Ellysse Dick, 'Schrems II': What Invalidating the EU-US Privacy Shield Means for Transatlantic Trade and Innovation' (Information Technology and Innovation Foundation, 2020) <https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/> accessed 11 March 2024.

2.4 Failures of previous transatlantic agreements on data transfer

Agreements on Data transfer between the EU and the U.S. have an extended and complex history of common commitments to reach a valuable solution. On one side, the privacy and data protection principles have taken a market-oriented approach in the United States. Instead, as we already analysed the GDPR is based on non-negotiable fundamental rights that must be guaranteed. Nevertheless, the United States considers its differentiate approach depending on the sector of application of privacy regulation was crucial for the success of American technological innovation, not over-regulating the business landscape. Therefore, a brief historical context of the previous agreements is required to comprehend the standoff in which we are today.

2.4.1 The Safe Harbour Agreement and Schrems I

Following the adoption by the European Union of its Data Protection Directive in 1995, the U.S. and the EU started an effort to establish a framework that would allow U.S. firms to fulfil adequate level of data protection required by the directive to avoid interruptions in personal data transfers from the EU.

The negotiation resulted in The Safe Harbour Privacy Principles[37], established by the U.S. Department of Commerce in 2000. The European Commission recognized that U.S. companies that were compliant with these principles would meet EU requirements for transferring personal data outside of the EU.[38] The Safe Harbour agreement, allowed a company or organisation in the United States to voluntarily issue self-certification to the Department of Commerce on a yearly basis to ensure its compliance with the adequacy decision. That would imply the respect of seven basic privacy principles, among which: *notice, choice, onward data transfer, security, data integrity, access, and enforcement, other than related requirements deemed necessary to meet the EU's data protection adequacy standards.*[39]

The FTC implemented the agreement, classifying any infringement of the Safe Harbour Privacy Principles as misleading activity according to Section 5 of the Federal Trade Commission Act banning "*unfair or deceptive acts or practices in or affecting commerce.*"[40] In addition, to ensure that the companies would continue to attain their voluntary self-certification every year they were obliged to re-register with the

[37] U.S. Department of Commerce, Safe Harbor Privacy principles of 21 July 2000, <https://rm.coe.int/16806af271> accessed 11 March 2024.
[38] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7.
[39] Archick and Fefer (n 20).
[40] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 section 45.

Department of Commerce, which contained a registry of all the organizations compliant with the Safe Harbour.[41]

However, not everyone was pleased with the safeguards put in place. Some Safe Harbour detractors sustained that the deal was simply a "minimalist solution" and that the U.S. never meant to follow on its promise to increase safeguards in the future.[42] Others underlined the FTC's lack of enforcement capabilities, which had not launched an enforcement case until 2009. Therefore, it was argued that these flaws demonstrated the agreement's incapability to guarantee meaningful data protection for EU citizens.[43] Moreover, the Snowden leaks, which encompassed allegations of extensive internet data surveillance by U.S. intelligence authorities, only served as the last step to erode the European Union's confidence in cross-border data exchanges with the U.S. Indeed, the revelations regarding the National Security Agency's (NSA) programs such as PRISM and UPSTREAM had a strong impact on the European Union, encouraging EU data protection law reform while negatively damaging trust in cross-border data flows.[44] The NSA through PRISM had access to sensitive information such as emails, documents, or photos from different American tech companies among which Google, Facebook, Apple, and Microsoft.[45] Moreover, via UPSTREAM the NSA was directly accessing communications made over fiber cables and communication infrastructure, in addition, such surveillance tactics may be implemented without a warrant if the collected data were related to foreigners located on the other side of the Atlantic.[46] Such actions were possible under the Foreign Intelligence Surveillance Act, known as FISA, which focuses on the capabilities of the U.S. government's collection of foreign intelligence data in order to bring forward U.S. counter-intelligence objectives. In particular, Section 702 FISA permits the U.S. authorities to search, collect, and process foreign intelligence data from foreigners situated outside of U.S. territory and jurisdiction without a warrant.[47]

Therefore, under those circumstances in October 2015 a judgment of the European Court of Justice (CJEU) invalidated the Safe Harbour Agreement. The judgment is known as Schrems I.[48] Indeed, the CJEU ruling originated from a complaint filed by an Austrian

[41] Mike Ewing, 'The Perfect Storm: The Safe Harbor and the Directive on Data Protection' (2001) 24 Houston Journal of International Law 315.
[42] W Gregory Voss, 'The Future of Transatlantic Data Flows: Privacy Shield or Bust?' (2016) 19(11) Journal of Internet Law 1.
[43] McKay Cunningham, 'Complying with international data protection law' (2016) 84 U Cin L Rev 421.
[44] ibid.
[45] Glenn Greenwald and Ewen MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' *(The Guardian*, 7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 11 March 2024.
[46] Craig Timberg, 'NSA Slide Shows Surveillance Of Undersea Cables' (Washington Post, 10 July 2013) <https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html> accessed 11 March 2024.
[47] Peter Margulies, 'Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on US Surveillance Policy' (2015) 72 Washington & Lee Law Review 1283.
[48] Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* ECR 650.

law student, Maximillian Schrems, with Ireland's Data Protection Authorities. Schrems complained about Facebook's transfer of his data from its EU-based servers in Ireland to its U.S.-based servers. In light of the 2013 exposures of U.S. NSA surveillance activities, Schrems filed several complaints with Ireland's DPA affirming and claiming that it was not present concrete protection against intelligence surveillance intrusion in US privacy law. Even though Schrems' complaint was dismissed by Ireland's DPA, the Irish High Court sustained his appeal and referred the issue to the CJEU. The court said that before concluding that the Safe Harbour principles guaranteed an adequate level of protection for EU individuals' personal data, the European Commission did not investigate properly into U.S. domestic legislation or international commitments.[49]

In particular, as well noted by Kuner the CJEU found that *Facebook's commercial transfer of personal data to the U.S., followed by further processing by U.S. public authorities for national security purposes, and combined with a lack of mechanisms for E.U. citizens to raise concerns to obtain redress, resulted in Safe Harbour failing to provide essentially equivalent protection as required by EU law in its Data Protection Directive and according to European Union Charter of Fundamental Rights (EUCFR)*.[50] Therefore, permitting U.S. authorities to interfere with personal data of citizen transferred across the Atlantic.

In particular, around 4,500 enterprises and organizations based their practice upon the Safe Harbour framework, therefore an immediate stop to the transfer of data could be disastrous for EU-U.S. economic ties. However, the EU declared a grace period of 4 months during which the outcome of Schrems I was not enforced. Thus, U.S. and EU officials could negotiate a new deal.[51]

2.4.2 The Privacy Shield and Schrems II

In February 2016, the negotiation between the U.S. and the EU gave its outcome, the EU-U.S. Privacy Shield was adopted. The newly established agreement was supposed to guarantee to companies the transfer of EU citizens' personal data to the U.S. while adhering to the requirements listed by the CJEU when it declared Safe Harbour invalid in 2015.[52] However, since the beginning the proposal announced was criticised in the EU, doubts were presented on the capability of the agreement to provide adequate

[49] Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid' (Press release No. 117/15, 6 October 2015) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> accessed 11 March 2024.
[50] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18(4) German Law Journal 881.
[51] Article 29 Working Party, 'Statement of the Article 29 Working Party' Press Release, 16 October 2015 <https://ec.europa.eu/justice/article-29/press-material/press release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf> accessed 11 March 2024.
[52] Martin A Weiss and Kristin Archick, 'US-EU data privacy: from safe harbor to privacy shield' (2016) Congressional Research Service <https://sgp.fas.org/crs/misc/R44257.pdf> accessed 11 March 2024.

protection for EU data subjects, adding that if these issues were not resolved prior to the Privacy Shield's implementation, the agreement could be challenged in front of the CJEU.[53] Nevertheless, the Privacy Shield agreement included commitment from U.S. officials in the form of letters that U.S. government access to EU citizens' personal data would be limited, as well as redress mechanisms such as the establishment of a Ombudsman at the U.S. Department of State to receive complaints from EU citizens in case of misuse of their data by U.S. national security authorities.[54] In July 2016 the Privacy Shield entered into force after the grant of an adequacy decision by the Commission with the hope that it would constitute a reliable compliance framework to transfer personal data for commercial purposes across the Atlantic. The adoption of the adequacy decision on behalf of the Commission was accompanied by the conviction on both sides that Privacy Shield had much greater privacy protections and oversight mechanisms than Safe Harbour, other than containing several redress options and enhanced safeguards relating to U.S. government access to personal data. However, questions still remained whether the agreement would survive future legal challenges in front of the CJEU.

The Privacy Shield basic structure was comparable to the one of the Safe Harbour; it was built on principles derived from EU data protection law that corporations can voluntarily self-certify to, and whose compliance is monitored by the Federal Trade Commission and Department of Transportation.[55] Nevertheless, the Privacy Shield is more complex and structured than the Safe Harbour agreement. Indeed, the Privacy Shield required the respect of seven primary principles namely: (1) *notice to provide transparency to individuals; (2) choice allowing individuals to opt out; (3) accountability for onward data transfer when data is sent to a third party; (4) security to protect data collected, (5) data integrity and purpose limitation for personal data collection, (6) access of individuals to personal data collected Recourse, (7) enforcement and liability for compliance. In addition, the framework included 16 supplemental principles creating different obligations for the companies to comply with.*[56] While participation in the Privacy Shield framework was on voluntary basis, when a company joined the framework, it was obliged to comply with the principles embedded in it.

[53] Article 29 Data Protection Working Party, 'Opinion 1/2016 on the EU-US Privacy Shield Draft Adequacy Decision' <https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2016/wp238_en.pdf> accessed 11 March 2024.
[54] European Commission, 'EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield' (Press Release, 2 February 2016) <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216> accessed 11 March 2024.
[55] Article 29 Data Protection Working Party (n 53).
[56] EU-US Privacy Shield Framework <https://www.privacyshield.gov/eu-us-framework> accessed 11 March 2024.

Moreover, an annual joint evaluation of the program could be conducted by the European Commission and the Department of Commerce, with experts from U.S. national intelligence authorities and European DPAs.[57]

Moreover, every European citizen had a variety of redress options under the Privacy Shield. Individuals could file complaints directly to companies or EU DPAs, which could submit unresolved concerns to the FTC. If the FTC declines to pursue a claim, Privacy Shield provided claimants with a free alternative dispute resolution mechanism. Indeed, a Privacy Shield Ombudsman was created to handle complaints about possible access and exploitation of EU citizens' personal data by U.S. national intelligence authorities. Although the Ombudsman was independent from the intelligence agencies, he is authorized to investigate matters referred by EU DPAs.[58]

Therefore, the Privacy shield at first instance assured more protection of the data of European citizens under many aspects, offering diverse means of redress and stronger data protection mechanisms. However, such efforts were not considered appropriate and sufficient to offer an adequate level of protection to European data in the United States territory. Indeed, a closer analysis of the new system reveals no significant upgrading in effective administrative and judicial redress for data subjects that have their data transferred.[59] In Schrems II, the CJEU broadly followed the pattern that used in Schrems I, indicating that a corporation to undertake business in the EU had to ensure adequate protection of data under EU law even when the data is transferred.[60] As a consequence, the Privacy shield after just four years into force has been invalidated by the CJEU judgment, known as Schrems II.

Since the CJEU's Schrems I decision invalidating Safe Harbour in 2015, Facebook Ireland announced that it was transferring most of its data to its U.S. servers via standard contractual clauses (SCCs), according to article 46 GDPR. SCCs are standard contract provisions that the EU 'pre-approve' to ensure that data transferred is protected according to EU standards. Therefore, Maximillian Schrems brought a new claim with Ireland's Data Protection Authority, inquiring the capabilities of SCCs to provide an adequate level of data protection, given the fact that U.S. surveillance laws could grant U.S. authorities access to personal data transferred to Facebook servers in the U.S. The case was brought to the High Court of Ireland, which then submitted doubts regarding the legitimacy of SCCs to the CJEU.[61]

[57] 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 [2016] OJ L207/1.
[58] European Commission, 'Guide to the EU-U.S. Privacy Shield' (2016) <https://ec.europa.eu/newsroom/just/items/605819> accessed 11 March 2024.
[59] Elaine Fahey and Fabien Terpan, 'Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield' (2021) 28 Indiana Journal of Global Legal Studies 205.
[60] Case C-311/18 *Maximillian Schrems v. Data Protection Commissioner* ECR 559, para 186.
[61] Xavier Tracol, '"Schrems II": The return of the privacy shield' (2020) 39 Computer Law & Security Review 1.

In the judgment issued in July 2020, although Advocate General Saugmandsgaard Øe suggested that the legal validity of the Privacy Shield was not needed of evaluation and ruled upon, the CJEU believed otherwise.[62] The Court considered the legality of the Privacy Shield decision in light of the GDPR's requirements, as well as Article 7 of the Charter's right to respect for private life, Article 8 of the Charter's right to personal data protection, and Article 47 of the Charter's right to effective judicial protection.[63] The two main takeaways have been: that the Privacy Shield framework could not be considered valid for transferring personal data from the EU to the U.S. given the breadth of data collection powers authorised in U.S. electronic surveillance laws and the lack of redress options for EU citizens. Indeed, the Ombudsman did not offer any guarantee of its independence from the executive, nor its capabilities to adopt decisions that are binding on U.S. intelligence agencies. It follows that the adoption of President Barack Obama's Presidential Policy Directive No. 28 (PPD-28)[64] which aimed to place limits upon U.S. surveillance powers was not instrumental to reassure the European counterparts. Indeed, the European Court sustained that the U.S. framework was lacking both an independent check on U.S. surveillance practices and sufficient and specific limits on surveillance's scope.[65]

The CJEU found in particular that Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, which allow intelligence services to gather more information than is strictly necessary, allow the collecting of more information not respecting the principle of proportionality enshrined in European law.[66]

The Grand Chamber's decision had sweeping practical repercussions. Indeed, a research conducted by the International Association of Privacy Professionals showed how SCCs were used by 88 percent of enterprises that transfer personal data outside of the EU, while the Privacy Shield was used by 60 percent.[67] Indeed, over 5,300 firms used the Privacy Shield standard for transatlantic data transfers, including digital giants Google, Facebook, Amazon, and Twitter.[68]

The invalidation of the Privacy Shield and the doubts about the legitimacy of the SCC brought confusion among businesses that formerly relied on it. Therefore, a new

[62] Case C-311/18 *Maximillian Schrems v. Data Protection Commissioner* ECR 559, Opinion of AG Saugmandsgaard Øe, paras 174-186.
[63] Xavier Tracol (n 61).
[64] The White House, Presidential Policy Directive/PPD-28, Signals Intelligence Activities, (Office of the Press Secretary 2014) <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> accessed 11 March 2024.
[65] *Maximillian Schrems v. Data Protection Commissioner* (n 62) paras 183-184.
[66] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 184.
[67] IAPP-EY, Annual Governance Report (2019) <https://iapp.org/media/pdf/resource_center/IAPP_EY_Governance_Report_2019.pdf> accessed 11 March 2024.
[68] William A Reinsch and Isabella Frymoyer, 'Transatlantic Data Flows: Permanently Broken or Temporarily Fractured?' (Center for Strategic And International Studies 2020) <https://www.csis.org/analysis/transatlantic-data-flows-permanently-broken-or-temporarily-fractured> accessed 11 March 2024.

adequacy decision on behalf of the Commission was needed to resolve the situation permanently.

3 An Analysis Of United States Surveillance Law

The U.S. and the EU addressed the concerns raised by the CJEU in Schrems II. In order for the U.S. government to produce an effective and long-term solution, it was required to bring changes to its surveillance ecosystem in the U.S. In order to strike a balance between national security and privacy in order to be able to achieve an adequate level of protection regarding the processing of personal data in the U.S.[69]

As already noticed, the CJEU held in the Schrems II judgment that U.S. surveillance activities carried out under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 12333) do not provide "the minimum safeguards" necessary under EU law to fulfil the proportionality principle. The European judges concluded that surveillance carried out under such statutes "*cannot be regarded as limited to what is strictly necessary.*"[70] Therefore, the court strongly underlined the necessity of effective safeguards against disproportionate government access to European data as well as judicial redress.

Before examining U.S. surveillance law it is important to remember, as underlined in the previous section, that the two systems adopted different kinds of regulations with different interference capabilities according to their view of privacy as an aspect of dignity in the EU and privacy as an aspect of liberty in the U.S.

Firstly, in the discussion on the balance between national security and privacy, it's often supposed that the U.S. finds a balance in favour of national security, whilst the EU takes a more strict approach that prioritises the protection of civil liberties, as the privacy of the individuals.[71] Secondly, despite historical disagreements over privacy, EU-U.S. intelligence sharing and counter-terrorism cooperation were strengthened in the aftermath of 9/11[72], effectively putting EU privacy advocates on the backburner. However, the tendency to foster such cooperation and to side-lining privacy advocates has been halted with Snowden's revelations. Indeed, the balance between national security and privacy in Europe has shifted since then, and the political pendulum in Europe has swung back in favour of privacy activists.[73] Finally, the presence of mass surveillance programs does not constitute novel practices by itself. What is remarkable

[69] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2017) 56(4) Journal of Common Market Studies 751.
[70] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 184.
[71] Francesca Bignami, 'European versus American liberty: A comparative privacy analysis of antiterrorism data mining' (2007) 48 BC L Rev 609.
[72] Davor Jančić, 'The role of the European Parliament and the US Congress in shaping transatlantic relations: TTIP, NSA surveillance, and CIA renditions' (2016) 54(4) Journal of Common Market Studies 896.
[73] ibid.

and unparalleled today respect to the past is the extent and the degree of capability of U.S. electronic foreign intelligence practices thanks to technological improvements. As a result, a rigorous examination of the extent of current surveillance capabilities, and the explanations they draw and the debates they cause is urgently required.[74] Therefore, we might conclude that modern U.S. surveillance law is out of step with the current demands of civil society regarding civil liberties.

We are going to analyse the most relevant U.S. case law on the balance between national security and privacy; then we will revert our attention to the most relevant U.S. surveillance laws. In order to be able to say which are the laws that put at stake the long-standing functioning of a transatlantic data pact.

3.1 Case law as basis for the wide scope of U.S. foreign surveillance law

Although courts have enabled reforms in certain cases, their rulings in the subject matter are often a source of transatlantic divergence, since they constitute the legal basis on which the governments construct their legal framework and policies. In particular, in this section, we are going to analyse the U.S. cases on which the U.S. administrations have developed their surveillance policies.

When balancing national security and privacy, the United States legal frameworks guarantee protections under the Fourth Amendment which impose restrictions on the government regarding surveillance practices or wiretaps. However, the strictness of these rules differs depending on which sector the U.S. authorities are acting such as for law enforcement, that encompasses crimes and offenses, or for national security.[75]

The case of Olmstead v United States (1928) sparked the first controversy about the relationship between electronic surveillance and Fourth Amendment rights. The Court concluded in this decision that intercepting telephone communications did not constitute a search or seizure within the meaning of the Fourth Amendment since it did not require a physical trespass onto a person's property.[76] The Court's decision stimulated heated controversy since it allowed non-trespassory forms of electronic surveillance.[77] In other instances, such as Goldman v United States[78] (1942) and Lee v United States[79] (1952), the contradicting 'trespass doctrine' was confirmed, establishing

[74] Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker, 'After Snowden: Rethinking the impact of surveillance' (2014) 8(2) International political sociology 121.
[75] Peter Swire, 'US Surveillance Law, Safe Harbor, and Reforms Since 2013' (2015) 36 Georgia Tech Scheller College of Business Research Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709619>.
[76] *Olmstead v. United States* 277 U.S. 438 (1928).
[77] L Rush Atkinson, 'The Fourth Amendment's national security exception: its history and limits' (2013) 66(5) Vanderbilt Law Review 1343.
[78] *Goldman v. United States* 316 US 129 (1942).
[79] *Lee v. United States* 343 US 747 (1952).

for several decades the legal standard for surveillance activities at the cost of personal privacy.

As briefly cited in the previous section, in Katz v United States (1967) for the first time the Supreme Court overturned the trespass doctrine, finding that "*because the Fourth Amendment protects people, rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure*."[80] It was also ruled that any intrusion, also electronic, into a location in which a person detains a reasonable expectation of privacy might be an infringement of the Fourth Amendment.[81] Furthermore, FBI activities such as wiretapping was deemed 'unreasonable' since it was carried out lacking a lawful warrant.[82] As a result, in Katz a privacy-based approach to the Fourth Amendment was approved.[83]

However, it is important to take notice that the Court at the same time established the so-called 'national security exception doctrine' in footnote 23 by stating that "*whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security is a question not presented by this case*." Therefore, the U.S. government according to Atkinson welcomed such provision in the Katz case as a "judicial blessing of the national security exception" which detained an important influence on the construction of future surveillance practices.[84]

Moreover, the matter of controlling national security surveillance was eventually addressed in United States v United States District Court (1972), widely known as the 'Keith' case, in which the question of whether a warrant was required to access electronic communications for reasons of national security was addressed. While the government claimed that "*the surveillance was lawful, [even] though conducted without prior judicial approval, as a reasonable exercise of the President's power to protect national security*"[85], the Court ruled that the governmental surveillance activities for domestic national security goals could be carried only when complying with the warrant requirement. However, it was not expressly answered whether the warrant provision extended to cases involving foreign intelligence surveillance.

As a result, the District Court in Keith not only reaffirmed the existence of the national security exception doctrine, additionally, it demonstrated that there was a distinct difference between foreign security surveillance that remained under the control of the Executive, therefore free from oversight, and domestic security

[80] *Katz v. United States* (n 23) para 351.
[81] ibid para 361.
[82] ibid para 363.
[83] Paul J Larkin, 'The Fourth Amendment and New Technologies' (The Heritage Foundation 2013) <https://www.heritage.org/report/the-fourth-amendment-and-new-technologies> accessed 11 March 2024.
[84] L Rush Atkinson (n 77) 1380.
[85] *United States v. United States Dist. Ct.* 407 US 297 (1972).

surveillance that was subject to Fourth Amendment restrictions protecting the right to privacy.[86]

In addition, in United States v Truong Dinh Hung (1980), the U.S. Court of Appeals for the Fourth Circuit recognized the 'national security exception doctrine' for the first time. The Court agreed with the government that there is a foreign intelligence exception to the warrant requirement, emphasising that "*the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following Keith, "unduly frustrate" the President in carrying out his foreign affairs responsibilities.*"[87]

The judgments discussed above demonstrate that the U.S. courts often agreed and approved a national-security approach to the Fourth Amendment. It makes apparent that the Fourth Amendment rests upon a two-layer system that distinguishes between internal and foreign security surveillance. As a result, it treats U.S. and non-US citizens differently. Finally, privacy guarantees and safeguards for U.S. citizens may result limited.[88]

Therefore, on such stances, the U.S. government could adopt laws that allow them to intrude on the private sphere of foreign citizens, and that constitute the major reason for which an adequacy decision cannot be granted by the European Commission to the U.S. legal framework.

3.2 United States foreign surveillance law: section 702 FISA and Executive Order 12333

Understanding of the CJEU's approach in Schrems II requires a closer examination of U.S. foreign surveillance with a focus on Section 702 of FISA and EO 12333. The former and the latter are the two statutes through which the government conducts signal intelligence surveillance activities. The NSA outlines signals intelligence, or SIGINT, as "*intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems.*"[89] Therefore, giving a broad leeway of action to U.S. authorities in their surveillance activities. In addition, the legal framework governing intelligence operations in the United States has not been updated to consider new technological realities, there are even larger loopholes that expose

[86] Elizabeth Goitein and Faiza Patel, 'What Went Wrong with the FISA Court?' (Brennan Center for Justice 2015) <https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court> accessed 11 March 2024.
[87] *United States of America, Appellee, v. Truong Dinh Hung, Appellant. United States of America, Appellee, v. Ronald Louis Humphrey, Appellant*, US Court of Appeals for the Fourth Circuit - 629 F.2d 908 (1980).
[88] Francesca Bignami, 'The US legal system on data protection in the field of law enforcement Safeguards, rights and remedies for EU citizens' (2015) Study for the LIBE Committee, GWU Law School Public Law Research Paper No. 2015-54, GWU Legal Studies Research Paper No. 2015-54.
[89] National Security Agency, Signals Intelligence (SIGINT) Overview <https://www.nsa.gov/Signals-Intelligence/Overview/> accessed 11 March 2024.

Europeans and even U.S citizens to surveillance and leave them unprotected from a legal standpoint. Therefore, U.S. surveillance law put at stake the sustainment of a stable international data transfer agreement, while raising doubt on the protection of the rights and privacy of their own citizens.[90]

3.2.1 The Foreign Intelligence Surveillance Act (FISA): section 702

The Foreign Intelligence Surveillance Act (FISA) was adopted in 1978 in the aftermath of the 1970s surveillance scandals, among which was the Watergate affair.[91] It provides the legal basis for modern US foreign intelligence activities and programs. The FISA was enacted as a result of comprehensive Senate Committee investigations into the legality of domestic intelligence activities. The goal was to guarantee better protection of civil liberties by building up a barrier between intelligence collection and enforcement.[92] In addition, FISA created a special court known as the Foreign Intelligence Surveillance Court (FISC) which would have the role to approve or refuse orders enabling electronic surveillance of specific targets.[93]

Furthermore, the terrorist attacks of September 11th, 2001 drove national security at the top of the U.S. government's priority list, resulting in an overwhelming majority vote in favour of the adoption of the US Patriot Act.[94] The latter significantly changed FISA. It gave federal law enforcement and intelligence agencies greater capability to collect and exchange evidence obtained through wire and electronic surveillance.[95] Moreover, in 2008 the FISA Amendments Act, which comprehends the "infamous" section 702, allowed the collection of communications by foreign persons that utilise U.S. communications service providers. Originally FISA was created to regulate surveillance activities targeting individuals within the United States. Section 702 was intended to extend such capabilities for the acquisition of intelligence information on non-US citizens residing outside the U.S. but without guaranteeing the safeguards provided by U.S. law, which are only relevant to U.S. citizens under the original FISA.

Section 702 has been at the centre of criticism since it provides the legal foundation for NSA surveillance techniques by allowing the agency to target freely the communications of foreign targets, without a warrant for national security purposes.

[90] Axel Arnbak and Sharon Goldberg, 'Loopholes for circumventing the constitution: Unrestricted bulk surveillance on Americans by collecting network traffic abroad' (2015) 21(2) Michigan Telecommunications & Technology Law Review 317.
[91] Francesca Bignami (n 71) 617.
[92] Robert N Davis, 'Striking the Balance: National Security vs. Civil Liberties' (2003) 29(1) Brooklyn Journal of International Law 175.
[93] Laura L Donohue, 'Bulk metadata collection: Statutory and constitutional considerations' (2014) 37(3) Harvard Journal of Law & Public Policy 757.
[94] USA Patriot Act of 2001, Public Law 107–56 of 26 October 2001, 107th Congress.
[95] Charles Doyle, 'The USA Patriot Act: a legal Analysis' (Congressional Research Service 2002) <https://crsreports.congress.gov/product/pdf/RS/RS21203> accessed 11 March 2024.

Unlike conventional FISA requests, which require a specific court order, 702 just requires the FISC to approve a singular annual government certification affirming that its procedures for obtaining and processing information are in accordance with the statute.[96] It is thus reaffirmed that U.S. surveillance law does not treat U.S. and non-US citizens in the same manner.

Section 702 has been enacted with the scope of codifying different aspects of the Terrorist Surveillance Program (TSP), which was established outside of the FISA framework by President Bush in 2001, in the section there are a locational and a substantive element.[97] The executive detains the capabilities of targeting communications of people or companies "reasonably believed to be located outside the United States" under Section 702. Mobile phone numbers and email addresses are selected to collect such communications. Moreover, to be lawful targets for surveillance activities does not suffice just to be located abroad, indeed United States persons, encompassing both U.S. citizens and foreigners with a lawful permanent residency (LPRs) located outside U.S. territory, are not targetable. However, there are included 'one-end foreign communications' which allow targeting a communication where there is at least one foreigner, also if the other part is within the United States territory, a U.S. citizen, or an LPR.[98]

Consequently, the targeting of foreign persons and companies under Section 702 results in the accidental gathering of enormous volumes of data on U.S. citizens.[99] Both the NSA, and other national agencies, among which the FBI, send requests to the database, which can provide results about people in the United States.[100]

Officials in the United States may target such communications in order to gather foreign intelligence information. Section 702 defines *foreign intelligence information as any information on attacks on the United States, espionage, sabotage, international terrorism, or the proliferation of weapons of mass destruction. Additionally, it includes a more nebulous category related to information of foreign power or foreign territory linked to the conduct of the foreign affairs of the United States.*[101] The category 'foreign affairs' in particular shows that 702's targets might cover a wide range of instances and subjects.

It appears logical to assume that to handle the extensive coverage under section 702 the U.S. employs automated technologies such as machine learning to detect trends

[96] Robert Stein, Walter Mondale, and Caitlinrose Fisher, 'No longer a neutral magistrate: The foreign intelligence surveillance court in the wake of the war on terror' (2015) 100 Minnesota Law Review 2251.
[97] Neal Katyal and Richard Caplan, 'The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent' (2008) 60 Stanford Law Review 101.
[98] Emily Berman, 'When Database Queries Are Fourth Amendment Searches' (2017) 102 Minnesota Law Review 577.
[99] *United States v. Hasbajrami* 945 F.3d 641 (2d Cir. 2019), paras 661-62.
[100] Peter Margulies, 'Searching for Accountability Under FISA: Internal Separation of Powers and Surveillance Law' (2021) 104(4) Marquette Law Review 1155.
[101] USA Patriot Act of 2001 (n 94).

in the storm of digital information accessible globally.[102] AI approaches and in particular machine learning may employ deep-learning neural networks that allow to swiftly filter through various variables in large volumes of data.[103] Thus, the employment of such technologies is of real concern for the protection of people that can be targeted under such wide capabilities on behalf of U.S. authorities.

Indeed, despite their many advantages, machine learning models have several flaws. Some models may be trained on incomplete or improperly selected data, for example, can generate fragile decisions that ignore context. Indeed, such naive models pay too much attention to insignificant changes in inputs, which any normal human being would appropriately disregard. In the training of machine learning, even minor modifications might result in significant output changes.[104] Furthermore, due to the large number of variables that neural networks process, frequently ambiguous outcomes can be produced that transcend standard linguistic explanations.[105] Another issue in machine learning that is particularly relevant for surveillance practices is the inherent risk that automated techniques may reflect human biases.[106] As an example, there may be fewer photos of individuals of color in a data set used to "train" an AI model in face recognition, or the data set may not represent the entire diversity of facial features across the globe.[107] Therefore, because of the scale of U.S. monitoring, machine learning's flaws are particularly notable and demand our attention on both sides of the Atlantic. As cited above, the targeting of foreign persons under Section 702 leads to the acquisition of vast amounts of data. Lastly, while the targeting process under Section 702 can be subject of independent review, the extent of that review is restricted given the circumscribed annual approval by the FISC.

Therefore, critics of Section 702 in Schrems II focused on the following: first, a lack of constraints on the capabilities conferred to implement surveillance programs, and second, the lack of guarantees and redress mechanisms for non-US persons who might be the target of those programs.[108]

3.2.2 Executive Order 12333 and PPD-28

While FISA primarily covers surveillance activities implemented within the territory of the United States, another statute through which U.S. authorities conduct electronic

[102] Peter Margulies, 'Surveillance by algorithm: The NSA Computerized Intelligence Collection, and Human Rights' (2016) 68(4) Florida Law Review 1045.
[103] Ian H Witten and Eibe Frank, *Data mining: practical machine learning tools and techniques* (Elsevier 2005).
[104] Bita Darvish Rouani, Mohammad Samragh, Tara Javidi and Farinaz Koushanfar, 'Safe machine learning and defeating adversarial attacks' (2019) 17(2) IEEE Security & Privacy 31.
[105] David Lehr and Paul Ohm, 'Playing with the data: what legal scholars should learn about machine learning' (2017) 51 UCDL Rev 653.
[106] Ashley Deeks, 'High-tech international law' (2020) 88 The George Washington Law Review 574.
[107] Aziz Z Huq, 'Constitutional Rights in the Machine-Learning State' (2020) 105 Cornell Law Review 1875.
[108] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 180.

surveillance abroad is Executive Order (EO) 12333, which was enacted in 1981 by President Reagan.

Executive orders are directives issued by the President of the United States. Executive orders are usually intended to govern activities of Government officials and agencies, not private citizens. The authority of the President to issue executive orders is derived from statutes and Article II of the Constitution.[109]

Therefore, surveillance policies governed by EO 12333 are solely designed and implemented by the executive. EO 12333 grants the NSA capabilities to gather, store, analyse, and disseminate foreign signals intelligence information.[110]

Indeed, the types of information that may be gathered under EO 12333 are broader. Under section 702 information that can be collected is limited to the 'foreign intelligence information'. Therefore, as analysed by the Privacy and Civil Liberties Oversight Boards (PCLOB), such restrictions do not allow the unrestricted collection of information about foreigners under section 702 FISA.[111] In contrast, under EO 12333 the categories that limit the types of information that the government may collect on U.S. citizens do not apply to non-US citizens. Therefore, no explicit constraints are present.

EO 12333 is structured in three sections. The first sets the goals of US intelligence and allocates tasks and duties to the Intelligence Communities (IC)[112] constituent agencies. Part 2 of the Order describes the necessity for foreign intelligence information and sets out standards to strike a balance with the safeguards of the rights of U.S. citizens. It requires IC to implement specific measures for collecting, retaining, and disseminating information about US citizens, as well as the use of precise collection techniques, however not including non-US citizens. Part 3 discusses oversight and guides intelligence agencies on the implementation of the Order, defining the terms contained in the statute.[113]

Furthermore, EO 12333 governs internet surveillance when it is carried on foreign soil and does not fall within the definition of electronic surveillance as set out in FISA in 1978. According to the NSA, EO 12333 applies when surveillance is conducted

[109] John Contrubis, 'Executive Orders and proclamations' (Congressional Research Service 1999) <https://sgp.fas.org/crs/misc/95-772.pdf> accessed 11 March 2024.

[110] National Security Agency, Missions, Authorities, Oversight and Partnerships of 9 August 2013 <https://irp.fas.org/nsa/nsa-story.pdf> accessed 11 March 2024.

[111] Privacy and Civil Liberties Oversight Board (PCLOB), 'Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court' of 23 January 2014 <https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf> accessed 11 March 2024.

[112] The United States Intelligence Community (IC) is a federation of executive branch agencies and organizations that work together and individually to perform intelligence activities required for the conduct of foreign relations and the protection of the country's national security. For more detailed information about the composition of U.S.IC see 'Members of the IC' (Office of the Director of National Intelligence) <https://www.dni.gov/index.php/what-we-do/members-of-the-ic> accessed 11 March 2024.

[113] Privacy and Civil Liberties Oversight Board (PCLOB), 'Executive Order 12333' (Report 2021) <https://documents.pclob.gov/prod/Documents/OversightReport/b11b78e0-019f-44b9-ae4f-60e7eebe8173/12333%20Public%20Capstone.pdf> accessed 11 March 2024.

with different means around the world, mainly outside of the United States, when it does not fall within the scope of FISA.[114] Unlike FISA, EO 12333 surveillance does not rely on the cooperation of service providers. The technical details remain classified and opaque, but the NSA has revealed that at least it involves exploiting flaws in telecommunications infrastructure.[115] Another point of friction is the capabilities to conduct bulk collection under the Order. Bulk collection entails conducting surveillance without a specific target or other discriminants. According to the National Research Council it is a collection "*in which a significant portion of the retained data pertains to identifiers that are not targets at the time of collection.*"[116] Such kind of activity cannot be carried under section 702 FISA. However, foreign intelligence collection under EO 12333 allows the U.S. government to gather signals intelligence in bulk collection when it is deemed essential in consideration to "technical or operational considerations."[117]

Since the bulk collection is by definition conducted without any discriminants, there is a great risk that the government will even obtain lots of information about people who have no relationship to wrongdoing or foreign intelligence information. Therefore, the U.S. government was pushed to put in place strong protections to limit these dangers, since EO 12333 was issued as an executive order the executive branch could do such without Congressional action.[118]

Concerns regarding the volume and nature of intelligence collection under E.O. 12333 prompted President Obama to issue Presidential Policy Directive 28 (PPD-28) in January 2014. The latter has been the first public commitment of the US government to protect the privacy of non-US citizens. PPD-28 discusses the safeguards to be provided to non-US citizens in the context of U.S. signals intelligence programs.[119] The directive states that: "*signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.*"[120] Therefore, the PPD-28 goal was to articulate principles to determine why, whether, when, and how the United States may perform lawful foreign intelligence

[114] ibid.
[115] Richard Lawne, 'US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM' (Fieldfisher 2020) <https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups> accessed 11 March 2024.
[116] National Research Council of the National Academies, 'Bulk Collection of Signals Intelligence: Technical Option' (2015) 2-9 <https://www.nap.edu/read/19414/chapter/1#vii> accessed 11 March 2024.
[117] Presidential Policy Directive (n 64).
[118] Sharon Bradford Franklin, Lauren Sarkesian, Ross Schulman and Spandana Singh, 'Strengthening Safeguards After Schrems II: A Roadmap for Reform' (*New America*, 7 April 2021) <https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/> accessed 11 March 2024.
[119] Daniel Severson, 'American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Change' (2015) 56(2) Harvard International Law Journal 465.
[120] PPD-28 (n 65).

and counterintelligence activities. In particular, the directive considers the safeguards to be provided to non-US citizens. However, despite its lofty language, PPD-28 purported reforms essentially just formalize and incentivize already existing practices inside the U.S. Intelligence Community, with significant policy changes occurring only on the margins, ensuring that the IC continues to detain sufficient authority to maintain the status quo.[121]

Indeed, on one hand, PPD-28 limits the use of data collected from bulk monitoring to six designated purposes: *(1) espionage; (2) terrorism; (3) weapons of mass destruction; (4) cybersecurity; (5) U.S. or ally armed forces; and (6) transnational criminal acts*.[122] On the other hand, it just restricts the use of the data gathered in bulk, not the purposes for which data is collected in bulk. In practice, intelligence agencies can continue to collect large amounts of data for any foreign intelligence objective, and PPD-28 simply limits how the government can use the data once it is stored in official databases. Therefore, it does not resolve the issue of data collected about persons not linked with any of the foreign intelligence objectives.[123]

According to the U.S. government, PPD-28 constituted a significant safeguard for non-U.S. citizens' civil liberties.[124] However, the CJEU considered PPD-28's safeguards insufficient, because the NSA has withheld its power to gather bulk intelligence signals without a clear and specific target.[125] Such safeguards are deemed insufficient to protect European citizens against the bulk collection of data by U.S. authorities under EO 12333. Consequently, the CJEU's position is confirmed, U.S. bulk collection is not necessary, nor proportionate, and, neither Section 702 nor EO 12333 provides individual data subjects with a means to seek redress against U.S. authorities for surveillance abuses.[126] Therefore, the main reason for the failure of the previous transatlantic data agreement has been shown clearly.

4 Towards A Stable Digital Economy Or Unfolding A New Chapter In The Schrems Saga?

On 10 July 2023, the EU issued its adequacy decision based on the Data Privacy Framework (DPF) negotiated with the United States, constituting an important step

[121] Richard Lawne (n 115).
[122] PPD-28 (n 65) section 2.
[123] Privacy and Civil Liberties Oversight Board (PCLOB) (n 111).
[124] Alexander W Joel, 'The Truth About Executive Order 12333' (*Politico*, 18 August 2014). <https://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121/> accessed 11 March 2024.
[125] *Maximillian Schrems v. Data Protection Commissioner* (n 62) para 183.
[126] ibid paras 181-184.

forward for the appropriate functioning of the digital economy.[127] Following the analysis conducted above, the new agreement, like its predecessors, will almost certainly be brought in front of the EU judicial system where will face the scrutiny of European Judges. The disposition in the new agreement was negotiated to meet the EU's standards requirement set out in Schrems II namely:

- Ensuring that the collection of personal data for national security purposes is limited to what is strictly necessary and proportionate according to article 8 CFREU to pass the proportionality test enshrined in article 52 CFREU;[128]
- The independence of the new redress mechanism respects the European individuals' right to an effective remedy and to a fair trial, and, whether any new authority part of this mechanism has access to relevant information, including personal data, when exercising its mission and can adopt decisions binding on the intelligence services as required by article 47 CFREU;[129]
- Lastly, if a judicial remedy against this authority's decisions or inaction is present.[130]

Now let's analyse how the new agreement tackled the issues at stake. In the wake of extensive collaboration between the US and the EU, an agreement in principle was reached in 2022, reflecting a shared commitment to facilitating data flows while protecting individual rights and personal data.[131] The subsequent Executive Order signed by President Biden and accompanying Regulations set the stage for significant improvements with respect to the Privacy Shield.

Executive Order 14086 introduces binding safeguards delineating stringent limitations on US intelligence authorities' access to EU data, aligning with the necessity and proportionality standards articulated by the CJEU. In particular, the DPF restricts U.S. signals intelligence capabilities towards 12 'legitimate objectives'. In addition, the establishment of the Data Protection Review Court (DPRC), as an independent and binding authority, enhances the redress mechanism, addressing the CJEU's concerns regarding the lack of effective remedies.[132] Indeed, the creation of the DPRC answers to

[127] European Commission, 'Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows' (Press release 10 July 2023) <https://ec.europa.eu/commission/presscorner/detail/eN/ip_23_3721> accessed 11 March 2024.
[128] *Maximillian Schrems v. Data Protection Commissioner* (n 62).
[129] ibid.
[130] ibid.
[131] The White House, 'Remarks by President Biden and European Commission President Ursula von der Leyen in Joint Press Statement' (Press statement, 25 March 2022) <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/25/remarks-by-president-biden-and-european-commission-president-ursula-von-der-leyen-in-joint-press-statement/> accessed 11 March 2024.
[132] US Department of State, 'Executive Order 14086 – Policy and Procedures' (3 July 2023) <https://www.state.gov/executive-order-14086-policy-and-procedures/> accessed 11 March 2024.

the two-holding made in Schrems II bringing a new structure to provide redress in response to a complaint from an individual in a qualifying state. Now every European citizen has at his disposal a two-tiered redress mechanism. In the first tier, it is possible to lodge a complaint with the 'Civil Liberties Protection Officer' of the US intelligence community. In the second tier, EU individuals are able to challenge that decision to the newly created DPRC.[133]

The commission explained how the new court differentiates from the ombudsman present in the Privacy Shield.[134] It ensures that the members of the DPCR are selected outside of the U.S. government, are appointed on the basis of qualifications, and are independent of instruction of the government.[135] Moreover, the DPCR in the mandate to investigate complaints of EU individuals will be fully able to obtain relevant information from intelligence agencies and capable to issue remedial decisions. Therefore, it appears that the new DCPR structure, while taking a decision upon a challenge of a European citizen, is able to meet the relevant EU legal requirements for independence and effectiveness.

The European Commission, taking these developments into account, moved forward with the adoption of the DPF adequacy decision in July 2023.[136] This decision allows for the transfer of personal data from the EU to the U.S. through a certification system. U.S. companies committing to privacy principles can facilitate data flows without additional mechanisms like Standard Contractual Clauses. The DPF constitutes a step forward, ensuring safe data flows, legal certainty, and strengthening economic ties.

However, concerns persist about how the court will work in practice. Questions remain about how the US interprets "proportionate" access to data, the transparency of the DPRC, and the framework's effectiveness in addressing alternative avenues of data access.

In particular, one of the main concerns still remains Section 702 FISA and debate of its reform that is undergoing in the U.S., indeed the FISA was expected to expire at the end of 2023. As suggested by a study by the Center for Strategic & International Studies: "*FISA reform could help the United States shift away from its global reputation as a*

[133] Théodore Christakis, Kenneth Propp and Peter Swire 'The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC' (IAPP 11 October 2022) <https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/> accessed 11 March 2024.

[134] European Commission 'Question and answers: EU-US Data Privacy Framework' (2022) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045> accessed 11 March 2024.

[135] For the list of judges nominated see here: US Department of Justice 'Attorney General Merrick B Garland Announces Judges of the Data Protection Review Court' (14 November 2023) <https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court>.

[136] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023] C/2023/4745.

"digital Wild West" and move toward shared global leadership on privacy and civil liberties."[137] They suggested to Congress to consider codifying privacy safeguards already present in the DPF in a renewed version of the FISA.[138] However, for the moment the validity of FISA was merely extended to April 2024,[139] whether the Act will be modified or not will be an important point of interest for the Commission for the annual review of the DPF.

However, it is also important to point out the recent case law of the CJEU on matters of surveillance, bulk collection, and data retention. In the past years, the CJEU shifted its approach regarding matters of surveillance capabilities on behalf of public authorities. From a first wave of fierce opposition to surveillance practices – with cases such as Digital Rights Ireland[140], the Schrems Saga, and Privacy International[141] – to a more pragmatic and procedural approach to surveillance practice.[142] In particular in La Quadrature du Net[143] the CJEU shifted from a strict approach banning completely surveillance practice to a more nuanced approach setting a list of lawful data retention practices that can be undertaken by national authorities.[144]

Therefore, the recent case law suggests that the CJEU may detain a less restrictive approach to the scrutiny of possible challenges to the DPF regarding U.S. surveillance capabilities.

For the moment Max Schrems contends that the DPF bears resemblance to its predecessors, indicating a potential legal challenge akin to 'Schrems III', that would probably reach the CJEU by Early 2024.[145] The European Data Protection Board (EDPB)[146] and the European Parliament (EP)[147] have also expressed reservations, emphasizing

[137] Caitlin Chin-Rothmann, 'Reforming Section 702 of the Foreign Intelligence Surveillance Act for a Digital Landscape' (Center for Strategic & International Studies 2023) <https://www.csis.org/analysis/reforming-section-702-foreign-intelligence-surveillance-act-digital-landscape> accessed 11 March 2024.
[138] ibid.
[139] Barbara Calderini, 'Gli Usa rinnovano la sorveglianza globale, ecco perché ci preoccupa' (Agenda Digitale, 29 December 2023) <https://www.agendadigitale.eu/sicurezza/privacy/usa-sinfiamma-il-dibattito-sulla-sorveglianza-dopo-la-proroga-delle-norme-antiterrorismo/> accessed 11 March 2024.
[140] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ECR 238.
[141] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* [2020] OJ C 433.
[142] Maria Tzanou and Karyda Spyridoula, 'Privacy international and quadrature du Net: One step forward two steps back in the data retention saga?' (2022) 28 (1) European Public Law 123.
[143] Joined Cases C 511/18, C 512/18 and C 520/18 *La Quadrature du Net and others v Prime Minister and others* ECR 791.
[144] Tzanou and Spyridoula (n 142).
[145] 'European Commission Gives EU-US Data Transfers Third Round at CJEU' (NOYB 10 July 2023) <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> accessed 11 March 2024.
[146] European Data Protection Board 'EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain' (28 February 2023) <https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en> accessed 11 March 2024.
[147] European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-U.S. Data Privacy Framework (2023/2501(RSP)) [2023] OJ C/2023/1073.

concerns about the adequacy of safeguards and the potential for legal invalidation by the CJEU. The Parliament points out that: "*the EU-U.S. Data Privacy Framework fails to create essential equivalence in the level of protection; calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU*".[148]

Therefore, despite the progress the path to a stable transatlantic data transfer framework remains complex. The Commission continuously monitors development in the US and will conduct its first review in July 2024. It will be a first watershed moment in order to understand how the agreement worked in practice and to grasp future implications.

While privacy concerns are valid, drawing premature conclusions might be counterproductive. A 'Schrems III' scenario, with another legal battle in front of the European Court of Justice, would only come with more uncertainty for EU individuals. While we navigate this evolving landscape, cautious optimism and a keen eye on the Commission's upcoming review seem prudent.

In this paper, we aimed to offer an understanding of past legal precedents, coupled with a forward-looking perspective, which will be crucial in determining whether the DPF heralds a stable digital economy or unfurls a new chapter in the Schrems saga.

5 Conclusions

The evolution of EU-U.S. data transfer agreements shows a continuous struggle to reconcile disparate perspectives on privacy and data protection. The new Transatlantic Data Privacy Framework demonstrates an effort to bridge the transatlantic privacy divide. It offers a potential solution to the challenges posed by the previous diatribes. Therefore, it was beneficial to reflect on the lessons learned from the failures of its predecessors.

The historical differences in privacy approaches between the EU and the U.S. are rooted in distinct legal frameworks and cultural nuances. Those differences have underscored the complexity of achieving a long-term transatlantic data transfer mechanism. The Privacy Shield and its predecessor, Safe Harbour, faced important challenges due to divergent surveillance laws and insufficient safeguards against U.S. intelligence intrusions, leading to their eventual failure.

The concerns raised by the Court of Justice of the EU in the Schrems II case highlighted the need for robust safeguards against government surveillance, sparking

[148] ibid point 19 of the resolution.

renewed negotiations and the development of the Transatlantic Data Privacy Framework. The framework, ushered by Executive Order 14086 and accompanying regulations, introduces binding safeguards and establishes a Data Protection Review Court to address privacy complaints.

However, the journey towards a stable and reliable transatlantic data transfer mechanism is far from over. Despite the improvements brought by the new framework, uncertainties persist. Questions surrounding the interpretation of "proportionate" access to data by U.S. authorities, the composition of the Data Protection Review Court, and the framework's ability to address data accessed through alternative avenues remain unresolved.

Privacy activist Max Schrems and others argue that the new framework echoes the shortcomings of its predecessors and falls short of instigating substantial changes in U.S. surveillance law. The concerns expressed by the EDPB and the European Parliament further underscore the need for vigilance.

The successful implementation and longevity of the Transatlantic Data Privacy Framework hinge on its ability to withstand legal scrutiny and address the core issues that brought down previous agreements. The recent nuanced approach of the CJEU on matters of data retention on behalf of public authorities may end up playing an important role in the matter.

The July 2024 review by the European Commission will serve as a pivotal moment to assess the framework's efficacy and adherence to EU legal standards.

With the looming possibility of a 'Schrems III', it remains imperative for both sides of the Atlantic to bear in mind the previous difficulties. Indeed, the quest for a durable and reliable transatlantic data transfer framework remains a work in progress, requiring persistent collaboration, mutual understanding, transparency, and a strong commitment to safeguarding the privacy rights of individuals on both sides of the Atlantic. Additionally, the actual international geological scenario reminds us that the Transatlantic partnership must be fostered in the midst of a future of uncertainty. Only through such efforts we pave the way for a safe and prosperous digital economy.

Journal of Law, Market & Innovation

ISSN: 2785-7867

https://www.ojs.unito.it/index.php/JLMI
email: editors.jlmi@iuse.it

The JLMI is edited as part of the
Open Access online scientific journals of
the University of Turin
Via Verdi 8, 10124
Turin, Italy

Vol. 3 - 1/2024