sustainability

MDPI

Article

Liable and Sustainable by Design: A Toolbox for a Regulatory Compliant and Sustainable Tech

Anna Aseeva

Legal Design GARDEN Association, 75010 Paris, France; anna.aseeva@graduateinstitute.ch

Abstract: The pandemic has exacerbated the effects of the digital transformation: the extractive economy is steadily giving way to the new economic space—the digital economy. This transformation shakes the very foundations of the existence and purpose of law, i.e., the regulation of social relations. However, today, the consequences of developing tech in an unsustainable manner are becoming obvious. Despite the internet's many benefits, it also erodes trust and fuels misinformation, polarization, and inequality. These developments occur partly because the algorithms that shape our economies, society, and even public discourse were developed with few legal restrictions or commonly held ethical standards. It is becoming increasingly obvious that the technologies that currently shape our socio-economic relations must be consistent with both our shared norms and values and the existing rules. The main question of this study is how to correctly introduce tech that is legal by design, but also, and especially, liable and sustainable by design. The underlying questions are hence, firstly: to this end, do we need (to create) a whole new body of norms, law, and regulation? Alternatively, are there already legal fields, concepts, and tools that can help us lay comprehensive groundwork for tech that is liable and sustainable by design? The central object of this study is to address this problem with regard to the types of organization that is in any way involved in or at least related to tech and innovation, essentially, the Web 3-4 actors. My principal method is systems analysis, which engages with a system as a whole. The construct of regulatory compliant and sustainable tech is thus analysed both functionally and institutionally, with concepts including norm-setting and law-making, formal application and enforcement, case law, real-world effects, and limitations. The objective of the article is to first synthesize the pre-existing legal and regulatory fields and constructs, and then analyse in a succinct yet systematic manner the conditions for their applicability to, and efficiency for, regulation of Web 3.0 (and soon, Web 4.0), as well as their limits. In the course of the study, I found that there are a few pre-existing legal fields, concepts, and tools that can pave the way to creating a Web that is liable and sustainable by design. I have also identified two key developments that arise from the digital transformation: (i) the digital economic space creates the so-called *governance and regulatory gaps*; and (ii) some of these gaps are rapidly filled (at times, successfully and at times, less so) by a burgeoning *newest legal framework* (national and supranational targeted regulation, legislation, and case law), which has been growing especially rapidly since the global digital 'leap' facilitated by the COVID-19 pandemic in the beginning of the 2020s. To conclude, the article summarizes both pre-existing and new tools and thus offers a ready-to-use toolkit for a regulatory compliant and sustainable tech (including a table summarizing the toolkit), which is the key aim of this paper.

Keywords: legal by design; digital economy; Web 3; web sustainability; sustainable digital ecosystem; tech & innovation law; startups; DAO; digital services; cyber-security; compliance; due diligence; data; GDPR; profiling; sustainable Artificial Intelligence (AI); generative AI; ChatGPT; EU AI Act; AI ethics; intellectual property for AI; NFTs; blockchain; cryptoassets; bitcoin

Citation: Aseeva, A. Liable and Sustainable by Design: A Toolbox for a Regulatory Compliant and Sustainable Tech. *Sustainability* **2024**, *16*, 228. https://doi.org/10.3390/su16010228

Academic Editors: Adam Smoliński and João Carlos Correia Leitão

Received: 13 August 2023
Revised: 17 October 2023
Accepted: 20 November 2023
Published: 26 December 2023

1. Introduction

The COVID-19 pandemic has exacerbated the effects of the digital transformation: the now-old global economic space, the extractive economy, is steadily giving way to the new economic space—the digital economy. This transformation shakes the very foundations of the existence and purpose of law, i.e., the regulation of social relations. For instance, the pandemic has pushed us all further into digital social spaces, putting questions of privacy at the forefront of societal regulation.

Today, the consequences of developing tech in an unsustainable manner are tangible. Despite the internet's many benefits, it also erodes trust and fuels misinformation, polarization, and inequality. That is partly because the algorithms that shape our economies, society, and even public discourse were developed with few legal restrictions or commonly held ethical standards.

It is becoming increasingly obvious that the technologies that currently shape socio-economic relations must be consistent with both our shared values and the existing legal and regulatory framework. Take, for instance, data protection. Confronting the abuse, exploitation, and manipulation of data collected via the internet is a *fundamental rights* issue (that is, the legal challenges related to these harvested data have implications for privacy and personal safety), as well as the one of *contract law* (e.g., limits to the freedom to operate) and *intellectual property rights* (e.g., copyright issues), etc.

In that regard, for example, the European Union's (EU) General Data Protection Regulation (GDPR) is today considered the world's strongest data protection law [1]. It regulates how individuals (and now, increasingly, algorithms) access and use personal data and draws boundaries between what organizations and businesses can and cannot do with our personal data [2]. Undoubtedly, the GDPR has introduced *privacy by design*.

The **main question** of this article is how to correctly introduce tech that is *legal by design*, but also, and especially, tech that is ***liable and sustainable by design***. The **underlying questions** of this paper are as follows. Firstly, to this end, do we need (to create) a whole new body of law and regulation? Alternatively, are there already legal fields, concepts, and tools that can help us lay comprehensive groundwork for tech that is ***liable and sustainable by design***?

I argue that lawyers and society at large already have a handful of legal concepts, ethical standards, and policy tools from the fields that pre-exist the digital economy and can be adapted to pave the way for its regulation. My **objective** here is hence to first synthesize the pre-existing legal and regulatory fields and constructs, and then analyse in a succinct yet systematic manner the conditions for their applicability to and effectiveness for Web 3.0 (and soon, Web 4.0) regulation, as well as their limits. I will do that with the aim of offering a ready-to-use toolkit for regulatory compliant and sustainable tech. The development of that toolkit is thus the key **aim** of this paper.

The central **object** of this study is the type of organization that is involved in or in any way related to tech and innovation, those being essentially Web 3-4 actors. As a main **method**, I use systems analysis, which engages with a system as a whole. The construction of regulatory compliant and sustainable tech is thus analysed both functionally and institutionally, using concepts including norm-setting and law-making, formal application and enforcement, case law, real-world effects, and limitations.

This article proceeds as follows. Section 2 analyses the existing concepts and most recent practices in corporate and contract law, governance, and regulation applicable to tech organizations. As Section 2 shows, beyond more 'traditional'—capitalistic—constructs of corporate and contract law, consumer contract law and the neighbouring legal concepts, for instance, raise questions about how to create a sustainable—i.e., safe, transparent, and trustworthy—digital market ecosystem. The discussions of compliance (Section 3) and data protection (Section 4) thus naturally follow Section 2. Additionally, when one speaks about data privacy, especially with respect to the advent and ever-growing use of algorithms, questions of ethics (Section 5) and intellectual property rights (Section 6) are unavoidable. Regarding algorithm-based transactions, many concerns are also

raised by the growing tendency to tokenize assets via blockchain (Section 7). Here, the existing monetary and financial regulations (and regulators) sometimes help and sometimes struggle to classify and manage the tokenization of existing assets. This process is even more complex regarding the newly created types of assets, content, goods, and services that are fully digital.

Consequently, while the previous sections of the article tend to confirm the main argument of this paper (that we already have many legal texts and practice, tools and concepts outside the digital economy that are nevertheless relevant and fit the toolbox for creating regulatory compliant and sustainable tech), this last section on finance and currency also highlights many controversial points and the general limits of the previous legal and regulatory constructs in application to this new online world. The Conclusion (Section 8) summarizes the key findings and suggests avenues for future work.

2. Corporate and Contract Law, Governance, and Regulation

Corporate law (or company law, as we mostly call it in civil law jurisdictions) provides for the registration, organizational form, legal personhood (and the very legal existence), ownership, control, and governance of an organization.

Since the evolution of the corporation in the late nineteenth century, the two general approaches to business (and especially, corporate) ownership have been the shareholder and the stakeholder models [3]. The shareholder model views the corporation as the private property of its *share*holders—that is, the owners of the shares of that corporation [4,5]. In this construct, the primary function of the business organization, as well as the responsibility of its managers, is to advance those owners' interests, which are, principally, to maximize their financial returns [6,7]. The literature usually labels this construct as either the property model (conceiving of the company as the property of shareholders) or the contract model (because autonomous shareholders freely contract in it) [4,8]. The stakeholder model views the business organization as a social institution, comprising, and therefore also serving the interests of, a wider group of its *stake*holders—that is, all parties who deal with the firm, such as creditors, investors, employees, customers, etc. Here, the company's primary purpose is to ensure that corporate transactions are beneficial not just to the stockholders, but to all its participants [7]. The stakeholder business model is often called the managerialist framework, the social-entity framework, or the institutionalist framework [7].

Both models of more classic business organizations are still 'internal' in the sense of the constituencies they address. Unlike the shareholder approach, the stakeholder model does consider the general social welfare and companies' social usefulness. However, despite being more inclusive, the stakeholder framework still primarily considers participants *in* a firm. However, the global and borderless nature of the digital economy easily implicates remote actors and environments, which, despite not dealing with a company in any meaningful way, are still directly and adversely affected by its activities.

Today, companies in the tech sector, be those startups or so-called Big Tech, obviously need a more 'external' approach to their purposes, governance, and accountability. This approach should extend an entity's accountability to all really and potentially impacted parties, including local communities and local natural or man-made environments (which are not necessarily regarded as stakeholders in most orthodox legal approaches), as well as society and the planet as a whole. This need arises because virtually all kinds of Web 3-4 businesses, especially startups, are, or should be, already in any way socially and/or environmentally useful, as today that is one of the sine qua non conditions that allow an innovation company, and, above all, a startup, to succeed.

Next, when dealing with financial products such as securities, tech firms are expected to be subject to the same rules as any firm (I discuss the tenets of the securities regulations applying to tech firms' *outputs* and *financial means* in Section 7 below). However, digital companies would most probably have to meet additional regulatory requirements.

The first point of attention for digital organizations is rooted in the field of corporate law and governance and concerns the new organizational forms taken by Web 3-4 entities that exist mostly—or even purely—online. This point is divided below into three analytical sub-points: (i) corporate status, (ii) contracting, and (iii) liability.

Let us take an example of a decentralized autonomous organization (DAO), a purely digital entity. A DAO is an organization with no central governing body whose members share a common goal of acting in the best interest of the entity [9]. The classical example of an early DAO is the *Ethereum* community [10]. One of the most typical forms of incorporation of DAOs is the LLC (Limited Liability Company), which is especially used for capital management, investment, and other such typical (crypto)financial activities [11].

The idea behind DAOs as organizations is to promote oversight and management of a business entity that is similar to a corporation [12]. It could be fairly said that a DAO is like and unlike a corporation, especially the above shareholder corporate model. It is like a stockholder-favouring company because a key preoccupation of the holders of its 'shares' (tokens) is to maximize their financial returns. Unlike a corporation or any kind of business enterprise based on the shareholder framework, however, a DAO's structure allows the tokenholders to participate in its management and decision-making in a bottom-up manner. This de-centralized management is an essential difference, but it is far from the only difference between DAOs and all previous forms of business organizations.

Popularized by cryptocurrency enthusiasts and blockchain technology, DAOs are primarily (but not exclusively) used to automate decisions in a blockchain and facilitate blockchain (especially, cryptocurrency) transactions [13]. DAOs have no central authority because their decision-making is distributed among tokenholders who cast votes in a collective manner [9]. After casting, all votes and any other DAO activity are posted on a blockchain, making all actions of its users completely transparent.

Another distinctive characteristic of DAOs is that they operate through smart contracts, logically coded agreements under which decision-making is based on underlying activity on a blockchain [12]. For example, based on the outcome of a decision, certain code may be implemented to burn a selected number of reserve tokens, increase the circulating supply, or issue selected rewards to current tokenholders [13].

Regarding corporate form and legal personhood, note that far from all jurisdictions recognize DAOs. Such jurisdictions as the Bahamas, the British Virgin Islands, the Cayman Islands, Gibraltar, the Marshall Islands, Panama, Singapore, and the states of Delaware, Vermont, and Wyoming in the United Sates (US) grant legal personhood to DAOs [14]. In Europe, Switzerland and Liechtenstein are to date the most popular destinations recognizing DAOs [14]. Within the EU, at the time of writing, Estonia and Malta give them legal personhood [15]. This list is frequently updated, so both the entrepreneurs wishing to open a DAO and organizations dealing with them in any way should constantly monitor this list in real time.

Secondly, and consequently, another important point of attention regarding new types of entities brought into existence by the digital economy such as DAOs is, as introduced earlier in this section, their (in)ability to contract. Indeed, in those countries where DAOs cannot have legal personhood, they naturally cannot act independently in contract proceedings. That is, since they cannot themselves enter into agreements, they are unable to sign a commercial contract, employ people, open a bank account, own assets, or even sign a lease agreement as an entity.

Creating a fully decentralized structure without any registered legal entity is also possible: it is chiefly done through decentralized finance (DeFi) ecosystems. In most jurisdictions, such DAOs are treated as general partnerships, which, in case of damage, will likely result in the personal liability of every participant. Some argue that such DAOs could legally own assets and hire staff because the participants create a fully recognized legal entity that can sue and be sued in court [16]. This point is debatable, and I address it below.

The above analysis leads to the third major pain point underlined earlier in this section—liability. Here, the issue of liability stems from tort law in those jurisdictions where

DAOs have no recognized legal personhood. Namely, corporate liability generally covers the extent to which a company as a legal person can be held liable for the actions of its managers and employees, including personal injury claims, corporate manslaughter, and corporate homicide [3]. This means that an employer is responsible for whatever its employees do, typically by negligence [3]. The tort of negligence and the tort of breach of statutory duty are the typical venues for such liability, however, DAOs with no legal personhood cannot be held liable in these venues on account of the above reasons. It is not obvious how such a DAO would be liable for damage, for instance, as, most probably, only the personal liability of the persons operating the DAO—its tokenholders—can theoretically be invoked. More research and practice are needed in that regard.

Another issue extends beyond DAOs to virtually any type of today's digital business and stems from the interface of consumer protection rules with contract law (also referred to as 'consumer contract law'). It relates to a difference between agreements at the professional (industry, that is) level, and those directed at final consumers—especially when we speak about natural persons, basically, you and I. Those agreements that are concluded between professionals and mainly directed to business and industry are called 'business-to-business' (B2B) contracts [17]. B2B contracts in the Web 3-4 sphere do not represent any particular challenge and are regulated more or less in the same way as B2B agreements in non-digital business relations. Nevertheless, in addition to these B2B contracts, firms, especially those in the retail sector, regularly enter into 'business-to-consumer' (B2C) agreements that are mainly directed at final consumers [17].

B2C contracts that are made with consumers online are often the mere general terms and conditions (of sale). They are regulated by the particular interface of contract law with consumer protection rules and are hence more difficult to draft and require more caution. At the EU level, the *Consumer Rights Directive* as well as its national implementations protect the consumers' side of the B2C contracts [18]. Notably, the former *European Unfair Contract Terms Directive* specified that unfair terms used in a consumer agreement by a sales operator (producer, supplier, retailer, etc.) are null and void and do not bind the final consumer, and it is essential to 'remove unfair terms' from such contracts 'in order to facilitate the establishment of the internal market and to safeguard the citizen in his role as consumer when acquiring goods and services under contracts which are governed by the laws of member states other than his own' [19].

Today, the *Consumer Rights Directive*, which consolidated pre-existing EU consumer directives (namely, the *Sale of Consumer Goods and Guarantees*, *Unfair Contract Terms*, *Distance Selling*, and *Doorstep Selling*), takes up these consumer contract law disciplines.[18]. The Directive constitutes part of a broader set of *EU Consumer Protection Acquis* [20] which tech companies should know and respect regarding matters relevant for B2C relationships. Otherwise, in this and connected matters, digital firms operating in the EU (or in any way directly related to the single market), should also be mindful of the *e-Commerce Directive* [21], adopted in 2000, as well as the *Digital Services Act* [22], which was adopted 22 years after the e-Commerce Directive and updates and complements it.

Hence, consumer protection rules and related consumer contract law are all the more stringent and require permanent follow-up in the constantly changing context of the digital economy and the regulation thereof. Indeed, since the COVID-19 pandemic, an ever-increasing number of goods and services are purchased online. Such purchases constitute the consumer's tacit consent to a sales contract. Especially relevant here are so-called contracts of adhesion [23]. Such a contract involves tacit, and often unwanted, consent on behalf of the consumer, particularly for 'beginners' in online purchasing [23]. Indeed, the simple click of a mouse allows the buyer to consent to the proposed contract on a website.

The legal principles governing the enforceability of unsigned B2C agreements vary according to national laws. Under the French Consumer Code, for instance, a contract is considered concluded only when a clear and precise offer is accepted without reservation. However, this offer-acceptance condition may be deemed unfulfilled if the buyer becomes aware of the 'shrink-wrap' contract's provisions only after the transaction is completed

[24]. Article L121 of the Consumer Code provides for a period of seven clear days; therefore, consent is formulated only at the conclusion of these seven days [24]. In the US, the Seventh Circuit Court considered that distance B2C agreements, such as, for example, 'shrink-wrap' agreements, are enforceable only if: (i) the packaging clearly indicates to the buyer that the good (a software, in that case) is licenced; (ii) the buyer is, or can easily become, fully aware of the conditions of the licence; and (iii) the buyer has the option to reject the contract by returning the software and obtain a refund [25,26].

Interestingly enough, in June 2023, a Canadian judge ruled that a 'thumbs-up' emoji represented B2C contract agreement [27]. Justice Timothy Keene of the Court of King's Bench in the province of Saskatchewan, who at one point used a *dictionary.com* definition of the symbol, concluded that the case "led the parties to a far flung search […] to unearth what a 👍 emoji means. […] (paragraph 30 of the judgment) [27]. This court readily acknowledges that a 👍 emoji is a non-traditional means to 'sign' a document but nevertheless under these circumstances this was a valid way to convey the two purposes of a 'signature'" (paragraph 63 of the judgment) [27]. It would probably have been more accurate to say that the 'thumbs-up' was actually an acknowledgement of receipt of a signed contract, rather than a *signature* to the contract. The conventional method of expressing consent to be bound by a legal agreement remains the signature of a duly authorized person. Be that as it may, with the Web 3–4, we have to adapt the existing rules to the new realities of the digital economy (and that is also exactly what Judge Keene said in paragraph 40 of the judgment) [27]).

Consequently, the correct drafting and application of B2C contracts, as well as close attention to the legal peculiarities of the related points such as the general terms and conditions of sale, the consumer protection rules in force in a given jurisdiction, and other constructs analysed above are crucial to allowing any online enterprise that sells or provides any kind of content, goods, or services to stay compliant.

3. Compliance

Regulatory compliance somewhat complements consumer protection. It often covers the sector-specific rules stemming from safety, security, and fundamental rights protections in the areas of anti-terrorism, prevention of various forms of abuse, anti-corruption, money laundering, etc. It is not really and not necessarily about tracing and/or controlling every step taken by consumers and a broader group of internet users. Rather, its main objective is to make a market more 'ecological', because a 'clean'—that is, organized and clear—market is a sustainable market, a safe and transparent ecosystem of trust, and therefore, a market that can develop.

Compliance rules often come from fields that pre-existed Web 3-4, such as banking and finance law and regulation, with such basics as KYC (Know Your Customer) and KYB (Know Your Business) information. These data comprise a client's or an investor's identity and/or fund verification procedures. Knowing the customers and business partners is key to ensuring that a market is not 'polluted', and only the service provider is able to carry out these checks. I will cover these and similar questions regarding not the *enterprises themselves*, but also and especially their financial and monetary *inputs/outputs* in Section 7, below.

When we speak about enterprises on the online market, it is important to make sure that their customers and/or business partners are 'ecological' in the sense that they provide safe and original content, goods, or services. For instance, an online marketplace, which is, along with DAOs discussed in the previous section, an increasingly typical example of a Web 3-4 business, will have to monitor and trace its traders in order to ensure a *safe, transparent and trustworthy ecosystem for consumers*. Organizing their *online interfaces* in a way that allows digital businesses to carry out their due diligence and information obligations towards consumers is another sine qua non feature of regulatory compliant online marketplaces and virtually all types of tech companies.

It is important to note that in the EU, public authorities are now able to remove unsafe content, products, or services directly from the online platforms [28]. EU operators of online marketplaces are also required to make reasonable efforts to randomly check whether unsafe content, products, or services have been identified as being illegal in any official database and, if they have, to take the appropriate action [28].

Under these new EU rules that function under the banner of the *Digital Services Act (DSA)*, which was already introduced in Section 2 above, entities running online platforms that are in any way accessible to minors are required to put in place appropriate measures to ensure high levels of privacy, safety, and security of minors on their services [22]. Furthermore, the DSA will also prohibit advertising that targets minors via profiling based on users' personal data when it can be established with reasonable certainty that those users are minors [22].

In addition to the EU DSA, which regulates the obligations of digital companies that act as intermediaries in their role of connecting consumers with goods, services, and content, an online operator who does not currently have a compliance programme will likely encounter considerable financial obstacles to finding a bank, a payment service provider, etc.

Overall, implementation of a compliance strategy for a tech organization involves a robust and well-thought-out risk management strategy. Once this strategy is ready, the enterprise must establish relevant procedures and ensure that its management, operations, and transactions comply with its strategy and promises, including public pleas (most typically, on the website of the company). Parts of such data must be made publicly available.

4. Data Governance

Beyond public data, *personal data*, as well as a clear information on how exactly an online operator gathers and manages such data, are today governed by increasingly strict regulations around the world [29–31] and are thus quickly becoming sine qua non conditions that any digital business must meet. There is also a growing body of court cases, for the moment chiefly targeting Big Tech firms (such as Amazon, Apple, Facebook (and Meta, more generally), Google, etc.) that makes governance of, as well as protection of internet users' personal data stricter every day [32–36].

As the GDPR is by far today's strictest data protection law, any digital business in any way related to the EU single market (such a relationship is quite global for obvious reasons) will have to establish a GDPR register and determine the purposes of data collection; the exact types of collected data; the retention periods; the recipients, including subcontractors; conditions of data transfer outside the EU, etc.

For instance, if an online business, say, a DAO, is registered in Switzerland as a Swiss legal entity (because, as we saw earlier, unlike most EU members, Switzerland fully recognizes DAOs), it will have to comply with the GDPR if it processes the personal data of individuals located in the EU, offers its services to EU citizens, and/or in any way monitors the behaviour of EU citizens. The GDPR will also apply to any Swiss-incorporated online business, not only to DAOs, if one of these conditions is met, and, in addition, if a company offers any goods or content to EU citizens (that is, does so on the EU market). Note that Switzerland recently adopted its own data protection law. The new Federal Act on Data Protection (nFADP) came into force on 1 September 2023 [29]. The most important difference between GDPR and nFADP is that in the EU, only companies are held liable for the data privacy-related issues described earlier in this section, whereas in Switzerland, any private data operator can now be found liable under nFADP and then fined up to 250,000 CHF [29].

This particularity of the new Swiss data law may in theory have some consequences for the liability of non-registered DAOs, as discussed in Section 2 above with respect to corporate and contract law. Imagine, for instance, a (obviously, non-Swiss incorporated) DAO that is based in a jurisdiction that does not grant it legal personhood. This DAO offers content, goods, or services on the Swiss market, processes the personal data of in-

dividuals located in Switzerland, and/or in any way monitors the behaviour of Swiss citizens. Unlike GDPR, nFADP will apply and will likely result in the personal liability of every participant of such a DAO, with possible fines up to 250,000 CHF.

What if a digital business does not collect personal data, but only wallet addresses or transactions? That might actually be the case for many DAOs, as well as of many kinds of the so-called FinTech startups and other types of business organizations, especially those working in one way or another with cryptocurrency. The main scenarios that are possible here are as follows. First, wallet addresses could be considered personal data insofar as they make a person identifiable. Hence, an entity must carry out the compliance measures related to identifying its customers (the KYC information discussed in Section 3 above). Second, if an entity does not itself do the KYC, the customers may create their wallet address on another platform (custodial wallet). In this case, the concerned online platform has to carry out the compliance measures.

Another crucial point with regard to data protection is the increased gathering, processing, and usage of data by last-generation artificial intelligence (AI), including the general-purpose AI models (such as large language models (LLMs), GPT-4, etc.). Take, for instance, the so-called legal intelligence platforms. They are supposed to help legal professionals automate a certain portion of their work, especially by (i) doing online legal searches (collection of legal documents) and (ii) creating comprehensive documents (enrichment thereof) [37]. These platforms' AI does these tasks by finding on the web and automatically highlighting crucial information, which is then enriched with relevant external data such as legislation, court rulings, commercial registries, etc. Most typically, one can find both the original and the enriched documents in the database of the platforms. Among these documents are *court decisions*.

With the *publication, enrichment (and eventual re-usage)* of court decisions, the main hurdle is an uneasy balance between (i) personal data and the overall privacy of each person mentioned in the decision, on the one hand, and (ii) public policy, and, specifically, the interests of the general public to access the court decisions, on the other [37].

With regard to privacy, the fundamental rights at stake are:

- right to privacy;
- right to personal integrity;
- in the context of 'sensitive' litigation, the risk of disturbances or reprisals following the publication of the judgments, particularly for decisions related to such issues as terrorism, family, etc., and hence, the right to avoid / interest in not suffering from these risks; and, finally,
- interest in not suffering the inconvenience of seeing one or more sensitive court decisions freely accessible on the internet (as a derivative of a right to digital/information self-determination).

On the opposite scale (public policy/ interest), at stake are:

- right to a fair trial;
- principle of publicness of court decisions;
- right to reuse public information;
- right to information; and
- freedom of expression.

First, the principle of pseudonymity, or concealment of personal data and information, postulates that court decisions are responsible, according to the practice and/or the regulations applicable to that court, for the initial concealment of information (typically, the surnames and first names of natural persons) before the platforms get these data. In such cases, the platforms receive only an already anonymized version of the decision.

Note that the GDPR provides for data minimization in court proceedings (GDPR Article 5(1)(c)). Additionally, the GDPR enshrines a pseudonymization (concealment) measure (GDPR Article 4(5)). The latter is limited to certain specified categories of personal data, which is a measure of security (among others) equally provided for in the GDPR

(Article 32). The application of these measures is to be proportionate to the risks associated with the processing. Unlike the GDPR's obligation to anonymize data, which is an obligation of result, pseudonymization is hence arguably an obligation of conduct (for the legal intelligence platforms, in the context of this analysis).

It is not possible to attain zero risk of breaching privacy in this context. However, if the online platforms comply with relevant EU law, it is very unlikely that there will be a substantive risk and significant harm to, or adverse impact on, the concerned individuals.

Moreover, regarding the interface of data privacy and publicity, on 2 March 2023, in the case *Norra Stockholm Bygg*, the CJEU ruled that

1. Article 6(3) and (4) of [the GDPR] must be interpreted as meaning that that provision applies, in the context of civil court proceedings, to the production as evidence of a staff register containing personal data of third parties collected principally for the purposes of tax inspection.
2. Articles 5 and 6 of [the GDPR] must be interpreted as meaning that when assessing whether the production of a document containing personal data must be ordered, the national court is required to have regard to the interests of the data subjects concerned and to balance them according to the circumstances of each case, the type of proceeding at issue and duly taking into account the requirements arising from the principle of proportionality as well as, in particular, those resulting from the principle of data minimisation referred to in Article 5(1)(c) of that regulation.'(paragraph 60, emphasis added) [34] .

Notably, this CJEU decision generally confirms the above analysis, in particular regarding the right to reuse public information.

Another current issue regarding personal data is *profiling*. Profiling could be delineated as the establishment of a probability concerning the ability of a person to access a certain service. When it is done on the basis of algorithmic decision-making, such establishment is said to be *automated* [36]. GDPR article 22(1), for instance, says that a person has 'the right not to be subject to' certain decisions. However, EU law scholars often assume that this right implies a prohibition (with exceptions) of such decisions [38–42].

In practice, profiling has recently been addressed by the CJEU in the case *SCHUFA Holding*. The Advocate General Mr. Prit Pikamäe said in his Opinion that the 'automated establishment of a probability concerning the ability of a person to service a loan constitute[d] profiling under the GDPR' [36]. The relevant parts of the Opinion make clear that being subject to profiling by AI constitutes profiling under the GDPR; it also means being subject to a decision having legal, socio-economic, and similar important consequences in this context. Importantly, AG Pikamäe stated that 'the GDPR establishe[d] a 'right' for the person concerned not to be subject to a decision based solely on automated processing, including profiling' [36].

Last, but definitely not least, the upcoming *European AI Act* is expected, among others, to protect and enhance the rights of EU citizens to file complaints about AI systems and receive explanations of decisions based on high-risk AI systems that significantly impact their fundamental rights [43]. The EU AI Act would also present an extensive list of prospectively prohibited AI practices, including bans on *intrusive and discriminatory uses of AI*, such as:

- 'real-time' and 'post' remote biometric identification systems in publicly accessible spaces;
- biometric categorization systems using sensitive characteristics, such as gender, race, ethnicity, citizenship status, religion, political orientation, etc.;
- predictive policing systems based on profiling, location, or past criminal behaviour;
- emotion-recognition systems in law enforcement, border management, the workplace, and educational institutions; and
- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases, in violation of human rights and the right to privacy [44].

Moreover, there is also a list of *high-risk AI applications*: AI systems that pose significant harm to people's health, safety, fundamental rights or the environment, or else AI that may influence voters and the outcome of elections and in recommender systems used by social media platforms (with over 45 million users) [44].

Under the prospective Act, providers of foundation models - a new and fast-evolving development in the field of AI—on the EU market would have to assess and mitigate all possible risks and *register their models in the EU database* before their release on the single market. Generative AI systems based on such models, such as ChatGPT, would have to comply with *transparency requirements* (disclosing that the content was AI-generated, also helping distinguish so-called deepfake images from real ones) and ensure safeguards against generating illegal content [44]. Detailed summaries of the copyrighted data used for their training would also have to be made publicly available [44]. AI data copyright and other intellectual property-related aspects are analysed in Section 6 of the article, whereas the current and prospective transparency and other due diligence requirements regarding AI-generated content (including deepfakes) are further discussed in the next section on ethics.

5. Ethics

In tech regulation, and, more broadly, in the digital economy, ethics is closely related to the above questions of data governance, privacy, and, specifically, AI-related proceedings. As said in the introduction, at present, the consequences of developing tech in an unsustainable manner are obvious: the digital economy, while facilitating our access to virtually any content, good, or service through the internet, may also erode trust and fuel misinformation, polarization, and inequality. Indeed, the algorithms that shape our current socio-economic relations were developed not only with few legal restrictions, but also, and, indeed, especially, with fewer commonly held ethical standards.

As, for example, the prospective EU AI Act's content, discussed in Section 4 above, demonstrates, it is becoming increasingly apparent and indispensable that the technologies that shape our current economy and society be consistent with our shared values and ethical standards.

In any matter related to data governance, privacy, and, particularly, the deployment of AI, today's tech organizations will have to conduct deeper ethical due diligence of their business partners, as well as screening of the content, product, and/or service they are offering, its impact on society, and the conditions that they will have to define ex ante to use/deploy it.

Today, one of the key ethical concerns regarding AI involves so-called deepfakes, which were already invoked in the previous section of this article. Deepfakes involve the manipulation of physical appearance, including human facial appearance, through deep generative methods [45]. It is needless to say that deepfakes can adversely affect our socio-economic relations, our everyday life, and society as a whole. They can be harmful, for example, in education and research (e.g., in plagiarism, transparency, lawful grounds for data processing), banking and finance (fraud, fake identities for bank accounts and financial proceedings, unlawful access to bank accounts, etc.), justice (administration and enforcement thereof), etc. [45].

Other ethical dimensions that a version of Web 3-4 that is *liable and sustainable by design* should be mindful of include, but are not limited to, secure and authentic information (so, questions of safety and privacy), a safe online space for everyone (questions of equality, and, to some extent, of safety), equal access to education, employment, and the social system, and, eventually, a market of goods, services, and content (questions of equality).

The latter question of equality of access is today directly relevant for tech companies and AI for several reasons. Specifically, the algorithms, especially, generative AI [46], bring more context to our online search results, help us write our software and create our applications, they communicate *with us* and/or *instead of us* in generating text, images,

code, videos, audios, etc. AI also creates new search engine architectures, serves as personalized therapy bots, assists developers in their programming tasks, and, through chat bots, assists us in our everyday interactions with virtually all providers of goods or services online [47].

The above benefits, however, also come with downsides and even dangers. The use of AI may involve abuse, exploitation, and manipulation of personal data collected via internet use. Algorithms are also increasingly used to make important decisions affecting all stages and areas of our life, from school and university admission, to job search, to loan application, to granting insurance and medical treatment, and beyond [47]. For example, today, dedicated private law companies provide credit institutions with a score assessing citizens by using their private data collected from the internet [47]. On account of this score (also called AI profiling, as defined in Section 4 above), though it is based solely on automated processing, credit institutions may make negative decisions (to refuse a loan application) that significantly affect people's lives [36]. Aside from the socio-economic and legal effects of this decision, this system obviously raises questions of access to the market—in this example, the credit market—hence also raising ethical questions of equality and the ethical and moral soundness of making a fully automated decision on such subjects.

Note that not only the access to credit market, but also the other areas of our lives in which decision-making is based on, or informed by, AI processing, discrimination occurs in the same way. Today, it ranges from, as said above, our school years, to retirement, and, eventually, death (because AI can also inform—or even completely form—decision-making on such types of insurance as life and funeral insurance, for example). Specifically, AI creates groups based on patterns and correlations in attributes, behaviours, and preferences of users, e.g., our:

- web history and web traffic;
- choice of browser (Explorer and Safari are 'preferred' by the algorithms over Chrome, Firefox, or Opera);
- social media and selling platforms' data;
- lowercase use or all-caps use;
- speed of page scrolling;
- clicking behaviour;
- picture pixels;

etc. [47].

Humans are thus classified into *new discriminated groups* that are arbitrary, human incomprehensible, and random. Thus, contrary to groups that previously—'traditionally'—suffered from discrimination based on gender, age, ethnicity, etc., these new groups (such as lower-case users or owners of bad-quality pictures or phones) are random because they are defined by *incomprehensible and unknown characteristics and boundaries* created and deployed by AI in a random manner [48–51].

These ethical issues of privacy, safety, and, increasingly, equality, are drawing greater attention from policymakers and lawyers, who manage these questions in a more legalistic manner, especially in the EU, especially in litigation (see various CJEU rulings and AG Opinions, in such cases as *Norra Stockholm Bygg* and *SCHUFA Holding*, discussed and cited in the previous section on data governance).

Hence, every digital organization will have to undertake a kind of a 'double screening', making sure that their business partners and their business respect basic common ethical values and standards while monitoring the myriad legislative and judicial developments on the subject-matter. Such monitoring will be necessary above all when the work of tech firms in any way relates to the EU and its single market, as the EU approaches many aspects of the digital economy in a particular, yet quite stringent, way.

EU also has its own ethical and legal considerations for another important regulatory aspect of tech developments such as AI—namely, the protection of intellectual property.

6. Relevant Intellectual Property Aspects

The classic definition of intellectual property (IP) is a set of the intangible products of *human* creative activity [52]. Notably, unlike real property and personal property, which are often protected by physical security devices, IP is chiefly protected by sets of enforceable legal rights granted to 'owners' or 'holders' [52].

Web 3, and even more so, the upcoming Web 4, are bringing about the heyday of IP rights in the digital economy and our everyday life through AI, NFTs, and today, increasingly, the metaverse [53].

AI-related IP questions can roughly be divided into those stemming (i) from the *input* data *for AI* and (ii) from the *output* data *of AI*. For obvious reasons, the most relevant type of AI, especially regarding output data, is generative AI, which is defined in the above section on ethics.

Along with classification AI, generative AI systems are based on machine learning and thus partly write and adjust themselves: these systems work through an iterative *training process* that passes vast amounts of data through the system [45]. The dependence of generative AI on datasets cannot be overestimated: it means that the *input* for the system—*sourcing training data*—is critical to its output [54]. When the data are personal data, privacy and data-protection law and ethics are crucial, as discussed in Sections 4 and 5 above.

In terms of IP law, data-containing material is protected by copyright and database rights. The legal issues raised by these two legal constructs for consideration by any AI operator are as follows. Firstly, data may be copyrighted. *Copyright* protects works of artistic or author expression (those are broadly defined and include such material and content as books, films, music/video recordings, and even computer software, databases, etc.) against unauthorized reproduction or distribution by third parties [52]. While it does not limit what material might be considered as *protectable artistic or author expression*, copyright does not extend to *functional* works or ideas [52]. Using copyrighted data without the consent of the rightsholder can amount to infringement of the copyright owner's reproduction right—that is, their right to control copying of the work [54].

Copyright protection of/in databases can separately and/or additionally be protected by *database rights* [55]. Databases can encompass websites, among other digital media, and thus, qualifying databases receive protection when there has been *substantial investment* in obtaining, verifying, or presenting the contents of the database [54]. If somebody extracts (including by either permanent or temporary transfer) or reuses all or a substantial part of the content (i.e., makes the content available to the public) of a protected database without the rights owner's consent, the database IP rights are infringed [54].

There are, however, some exceptions to both copyright and database IP protection that allow the use of the copyrighted work or database in the context of training AI. Firstly, the exceptions to copyright infringement include non-commercial research or private study, criticism, review and news reporting, or caricature, parody or pastiche—all of which are subject to a 'fair dealing' restriction, an exception to which is discussed below [46]. There are also related exceptions for text and data mining (TDM) and temporary copies. All these types of IP protection vary across jurisdictions and must be analysed depending on the country of the AI's operator, its market, etc.

With respect to database IP protection, a 'fair dealing' exception applies to databases that have been made available to the public (in any manner) [46]. Database rights in publicly available databases are not infringed by fair dealing with a substantial part of their contents provided that (i) the extraction is carried out by a person who is a lawful user of the database; (ii) the data are extracted for the purpose of illustration for education or research and not for any commercial purpose; and (iii) the source is referenced by the user who extracts the protected content. Defined in this way, however, this exception is unlikely to apply in a commercial context [46].

In sum, regarding the *input* data, the tech firms that offer and/or use generative AI should be mindful that when their AI has been—or might have been—trained on data that are protected by copyright or database rights or both, and none of the above exceptions

apply, those data must be validly licensed; if they are AI suppliers, they must make sure that they consider any relevant IP rights in full and with up-to-date information; if they are users of such AI, they must seek assurance on this point from the AI supplier [54].

The two types of IP protection that are the most relevant to the second item in the present analysis, namely, generative AI *output*, are *patents* and *copyright*. Copyright was defined above in the analysis of the *input* data. The patent, which is the earliest type (together with the trademark) of IP right, is defined as 'a set of rights granted to the inventor of a product or process which is 'new' (or 'novel'), involves an 'inventive step' (or is 'non-obvious'), and is capable of industrial application (or 'useful')' [52].

Regarding patents, in the EU, for example, inventions generated by AI are not patentable. In 2022, the European Patent Office (EPO) decided that a generative AI system cannot be regarded as an inventor: that is, on a patent application, the inventors have to be *persons with legal capacity* [56]. Neither an invention generated solely by an AI machine without human involvement, nor the owner of such an AI system, is entitled to a patent [56]. AI is rather considered a computer-implemented invention. The *European Patent Convention* does not provide patent protection for computer programmes; however, it can offer such protection for inventions involving software if the invention produces a technical effect serving a technical purpose [57]. One example might be an automated system processing physiological measurements to provide a medical diagnosis, such as a heart-monitoring apparatus using a neural network to identify irregular heartbeats [57].

Regarding the interface of copyright with AI output data, copyright protects (i) the so-called *entrepreneurial works* (films, sound recordings, broadcasts, and published editions) and (ii) original *LDMA works* (literary, dramatic, musical, and artistic works) [52].

Unlike patents, copyright does not require *novelty* [58]. Regarding entrepreneurial works, there is no threshold of *originality* either: for instance, sound recording protections extend only to a specific recording of a song and last for 70 years from the recording's creation [46]. It is argued that these rights could apply to generative AI outputs: for example, if AI generates a song and records that song in the process, the person who took the necessary steps to have the AI generate and record the song is likely to be the producer and would hence hold the copyright to the recording [46].

In contrast to entrepreneurial works, the copyrightability of LDMA works requires *originality*—i.e., the work has to be the author's own intellectual creation [59,60]. When an LDMA work is created by a human with the use of AI, if the work expresses original human creativity, the AI will be treated as a tool [61]. The work will receive copyright protection much like any other LDMA work, and the rights will belong to the human author [61].

The copyright's threshold of originality is important here because later in this section, it will also be relevant in a discussion of NFTs. Thus, originality refers to a particular type of relationship between the author of the work and the work itself [58]. The authors should still be mindful that the nature of the originality condition differs across jurisdictions.

In the EU, the necessary relationship exists only if the work is the *author's own intellectual creation* [62]. Regarding more specifically AI-generated creative works, it has recently been decided that EU copyright law does not grant copyright protection to such works. More precisely, the CJEU has ruled that copyrightability does not extend to computer-generated works; copyright protection requires some form of human input because it must reflect the author's personality [46]. Thus, a creative work that involves *assistance* from AI is protected, provided that the human input meets the originality requirement [46].

The baseline of the EU copyright law's applicability to computer-generated output is that purely AI-generated works or works generated by other automated processes lack any form of human input and are, as such, not eligible for copyright protection: an AI system or any other type of computer programme may be copyrightable, but any output they autonomously create would not be [46,63].

In contrast, current UK copyright law protects LDMA works generated entirely by computers, provided that the originality condition is met [64]. Generative AI may put this

originality requirement under pressure. Recall that, as outlined earlier in this section, machine learning systems are dependent on their training data: for example, an image-making generative AI might create a digital image of an object, but the output would be shaped by images of that object that were created by somebody else and that already existed in its training data [46].

As the analysis of copyrightability of computer-generated LDMA works has shown earlier in this section, at the time of writing it remains untested whether such works generated by AI would undermine claims to originality. After more than two decades of freedom of the internet, with free and open access to large numbers of pictures, photos, videos, and other visual, sound, and/or artistic content (the latter is fully classified earlier in this section in regard to LDMA and entrepreneurial works), non-fungible tokens (NFTs) are radically transforming the way these kinds of digital content are understood and regulated.

'Non-fungible' refers to anything that is unique and cannot be replaced [65]. 'Non-fungible tokens' are defined as assets that have been tokenized via a blockchain by assigning to them unique identification codes and metadata that distinguish them from other tokens [66]. Unique or collectible, original art works themselves or visual representations thereof, photos taken with one's camera or life stories, they have a value (actually, contrary to fungible tokens, which have *value* properly speaking, the value of NFTs, similarly to the AI input discussed above, lies in their stored content, and, hence, the *data*), and thus can be bought and/or exchanged [65].

For example, one could even tokenize their own image through the process described above (by assigning to it a unique identification code and metadata via a blockchain), and if anyone finds it worth spending their money on it, they will pay for such an NFT. Once rights are attached to that kind of content, NFTs can be traded and exchanged for fiat money, cryptocurrency, or even other NFTs—it will all depend on the value their owners and the market assign to them.

However, NFTs have no value without the rights associated with the content: that is, without a licensing agreement, assignment of IP and/or image rights, and, specifically in the case of NFTs, a *contract for the transfer of rights*. In a nutshell, NFTs' essential features are indivisibility, irreplaceability, and uniqueness [66]. Aside from acting as IP, their primary real-life purposes are to serve as academic title, artwork, music composition, gaming, utility, access to a service, e.g., a subscription, and even assets, such as stocks or shares [65].

Therefore, it is important for startups and tech organizations of any size, as well as innovation project leaders and authors of LDMA and entrepreneurial works, to know and understand their rights, to register and protect any intellectual property as soon as possible, and to design an IP strategy that includes NFTs. Indeed, recall that, in the case of an LDMA work created entirely by an AI, the originality requirement would be limited by the AI's training data: an AI might create a digital image of a bicycle, but it would be shaped by the images of bicycles created by somebody else and included in its training data. Protecting one's images of a bicycle or of anything else, particularly in the form of NFTs, involves assigning to them a unique ID and metadata, and, eventually, value.

Note that any crypto token, including cryptocurrency, is built upon the same underlying blockchain technology as are NFTs. Some NFTs are traded on cryptocurrency exchanges [67] and are thus also part of cryptocurrency exchange (the most famous of them being The Doge NFT [68]), but not the other way around. Cryptocurrencies are payment coins that have their own blockchains: Bitcoin (BTC), Ether (ETH), and Litecoin (LTC) are examples of cryptocurrencies that function on their own blockchains [69]. Crypto tokens, on the other hand, are created on blockchains developed by another entity: for example, Chainlink (LINK) and Uniswap (UNI) are tokens developed on the ETH blockchain [70].

Many NFTs can be purchased only with cryptocurrency, most of them with ETH, which makes the former a kind of a good and the latter a payment method for that good. As was said previously, cryptocurrencies are built using the same kind of programming as NFTs, but that is where the similarity ends. Like fiat (physical) money, cryptocurrencies are fungible because they store value and act as a medium to buy or sell goods. That is

already the topic of the next and last substantive section of this article: monetary and financial aspects of the regulation of cryptoassets.

7. Regulation of Cryptoassets

When one speaks about AI and other algorithms, NFTs, blockchain, and the regulation thereof, naturally one cannot avoid considering the regulation of cryptomoney and a broader category of cryptoassets. Such regulation plays a major, even critical, role in virtually any Web 3-4 project.

In legal terms, the monetary system and the regulation thereof refer to national currency and exchange-rate policies, and the financial system and its regulation encompass the creation and access to (trade in) credit that could be either national or international, or, more precisely, transnational [71]. In this section, I address some relevant legal and sustainability highlights of the first, monetary, dimension, specifically, its first part—national currency—while also looking at the second strand—the national and international financial system. I will also consider the connected tenets of tax law.

Note that over the last few years, many countries have been developing their central bank digital currency (CBDC)—digital tokens issued by their central banks—a 'crypto-version' of their national currency. For instance, in August 2023, the US [72] and Russia [73] conducted pilot studies before launching their national CBDCs. That is, unlike private cryptocurrencies such as BTC, a US CBDC would be issued and backed by the Federal Reserve, just like US fiat money—USD bills and coins [72].

Regarding all cryptoassets, and, particularly, private cryptocurrencies (basically, everything that is not official legal tender in a given jurisdiction), the first point is easy and quite obvious. If a tech firm, a collaborative innovation project, or even an individual author produces an entrepreneurial or an LDMA work, they might consider (or even should, if they can) tokenizing their work. If they create NFTs, these NFTs can be purchased, as said in the previous section, with cryptocurrency. Today, many NFTs can be purchased only with ETH, for example, which, unlike the above national CBDCs, is not considered money or currency and is one of the so-called private cryptocurrencies. Thus, the entity must have a digital wallet, and, more precisely, a cryptowallet (even more precisely, today, an ETH wallet for receiving payments for NFTs is advisable). Clearly defining the holder(s) of the key to the cryptowallet is thus a sine qua non step if an entity decides to, partially or totally, receive and/or issue payments in, or else save, invest in, etc. cryptoassets.

Thus, the next set of questions comes naturally: the taxes. With respect to tax law, there will be an obligation for the organization to enter in its accounting books the Value Added Tax (VAT) on cryptoassets with the values expressed in crypto, which will involve drawing up a balance sheet, etc. Here, it will be extremely important to know which cryptoasset has which status (i.e., currency or investment (here, further distinguishing between property and security, especially, in the US)) in the jurisdiction where the entity declares and pays its taxes.

This point brings me to the next concern, which stems from the important and ongoing debate around the regulation of private cryptocurrencies, their status, registration, the connected tax declaration, etc. Consider that, while BTC is not defined as a security in most jurisdictions, important cryptos such as ETH and Ripple (XRP), the second and third most valuable private cryptocurrencies, respectively, which today are the most widely used for payments and transactions of many kinds, are under significant pressure in many jurisdictions, primarily in the US.

The US Securities and Exchange Commission (SEC) has clarified that BTC is not a security: '[c]ryptocurrencies are replacements for sovereign currencies…[they] replace the yen, the dollar, the euro with bitcoin. That type of currency is not a security' [74]. However, with respect to XRP, in December 2020, the SEC filed an action against Ripple Labs Inc. (the creator of XRP) and two of its executives, alleging that they raised over 1.3 billion USD through an unregistered, ongoing digital asset securities offering [75]. The recent ruling of 13 July 2023 in the above case concluded that sales of Ripple's XRP token directly

to institutional investors violated the SEC's rules but offerings to retail investors on exchanges did not [76]. That is, Judge Analisa Torres of the US District Court for the Southern District of New York issued a split decision in which she found that XRP was 'not in and of itself a 'contract, transaction, or scheme' that embodies the *Howey* requirements of an investment contract' [77]. She essentially stated that such a transaction did not involve *investment contract securities* and thus that the XRP token at issue was not a security.

Note that, at the time of writing, the SEC asked a federal judge to ignore these parts of the ruling, saying the judgment did not square with existing securities laws and that it might appeal [78]. This case illustrates *three major points*. Firstly, the above ruling is singularly important not only for Ripple Labs Inc. and XRP holders around the world, but also for the larger digital assets industry and holders, as the SEC has long taken the position that nearly all tokens except BTC are, in and of themselves, investment contract securities [78]. Secondly, this case, and especially the SEC decision to appeal the judgment, show that today XRP itself (still), ETH, and any crypto except BTC are the focus of pressure from regulators—in the US, first of all, but also around the world.

Thirdly, and importantly, any cryptowallet owner must hence be mindful of, and must constantly monitor the status of, *all the tokens* in it, whether they are, or are likely in the near future (especially through keeping up-to-date with relevant regulations, case law, and other important decisions in their country and around the world) to be considered investment contract securities. This caution is necessary because the method of declaring and paying taxes, as well as the very nature of the tokens in any cryptowallet, will depend on the applicable law and relevant decisions by the authorities.

Notably, on 25 July 2023, Singapore's High Court has ruled that the *holder of a cryptoasset* has a legally enforceable *property right* recognisable by the common law. This ruling constituted the first time that a common law court made such a decision [79]. While the case concerned corporate fraud and theft from ByBit Fintech, what is important for the analysis here is that Justice Philip Jeyaretnam held that a cryptoasset, more precisely, the stablecoin USDT, is a *thing in action*, and is thus enforceable in Singapore via court orders and also capable of being subject to a trust [79].

Even the legal status of the oldest, biggest, and most expensive (but also, allegedly, the safest) private cryptocurrency, Bitcoin, varies widely across countries and over time. Consider that in June 2021, El Salvador adopted BTC as legal tender, becoming the first country to make it the official national currency [80]. In April 2022, the Central African Republic followed El Salvador [81]. A few countries have fully banned BTC use (such as Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, Vietnam, and the United Arab Emirates), while more than forty have implicitly banned it (e.g., China, Colombia, the Dominican Republic, Indonesia, Kuwait, Lithuania, Macau, Oman, Qatar, Saudi Arabia, and Taiwan) [82]. Moreover, Australian banks have closed down the bank accounts of operators of businesses involving BTC since the country's National Bank recognized it as too risky [83,84].

A few jurisdictions use Bitcoin in some payment capacity as a kind of exchange token, including Switzerland and the US; some US states (e.g., Colorado) and Swiss cantons (for instance, Zug) even accept tax payments in BTC [85,86]. It should be remembered, however, that at the federal level, the US Internal Revenue Service (IRS) classifies *cryptocurrency*, *including* BTC, as *property*, not currency [87]. Thus, the SEC's above claims that it considers BTC 'currency' rather mean that, contrary to its treatment of all other cryptos, and given the SEC's scope of competencies (securities), it merely does not treat BTC as *security*. This classification also means that the US central authority responsible for *taxes* says that, for tax purposes, BTC and any other cryptocurrency are *not currency*, but *property*, and thus, buying and selling cryptocurrency is taxable under US tax law.

In the UK, the situation is similar to that in the US, but with more nuances. Like the US, the UK does not classify cryptocurrency as money or currency. Thus, anyone who holds cryptocurrency as a personal investment in the UK will then be taxed on any profits realized on such assets. However, His Majesty's Revenue and Customs (HMRC) further

details in its *Cryptoassets Manual* how to file cryptocurrency taxes. HMRC distinguishes four categories of cryptoassets (i) stablecoins, which are cryptoassets with value pegged to that of fiat money or exchange-traded commodities, such as, for example, Tether (USDT) and USD Coin (USDC), which are pegged to the value of US dollar; (ii) exchange tokens such as BTC, which can be used as a mode of payment, (iii) security tokens, which have interests and rights in business, such as, for example, entitlement to shares in future profits; and (iv) utility tokens, which provide access to goods or services accessible via a platform, usually using distributed ledger technology (DLT) [87].

In the EU, Germany is seen as one of the most cryptofriendly member states in terms of taxation [88]. Under the *German Tax Acts*, BTC and all other cryptos are considered *private money*, whereas the German Federal Central Tax Office (BZSt) does not classify cryptocurrency as property, foreign currency, or legal tender. Actually, as Germany treats cryptocurrency as a kind of 'private money', its laws favour long-term, buy-and-hold investors: short-term capital gains from cryptocurrency or cryptoassets held less than a year are subject to income tax, while those held longer than one year are not subject to such tax, even if the asset increases in value; individually-held crypto is VAT-exempt, and assets held for over a year do not incur a tax liability on earnings [87]. Moreover, for natural persons, profits from cryptocurrency and cryptoassets of less than 600 EUR a year are exempt from taxation [87].

At the supranational level, in 2015, the CJEU decided that BTC transactions would be exempt from VAT [88]. On the regulatory front, in 2013, the *European Banking Authority* (EBA) warned EU consumers about the high volatility of BTC prices and the possibility of general fraud, as well as the possibility that their BTC exchanges could be easily hacked [89]. They thus warned of a need to regulate BTC [89].

In June 2023, the EU adopted the *Markets in Crypto-Asset* (MiCA) [90] and the (revised) *Transfer of Funds Regulation* (TFR) [91] regulations, which aim to regulate the cryptomarket in the EU, and, naturally (because the two instruments are EU regulations), to harmonize the regulatory framework for the cryptoasset market across the Union.

MiCA covers cryptoassets that are not currently regulated by the existing EU financial services legislation (primarily, MiFID II [92]), supports innovation and fair competition, and presents the requirements and limitations for those issuing and trading cryptoassets by laying down supranational rules on transparency, disclosure, authorization, and supervision of covered cryptotransactions [93]. The revised TFR binds cryptoasset service providers to accompany any transfer of cryptoassets with information on the originators and beneficiaries, thus applying the equivalent of KYC and due diligence obligations to the cryptoassets market within Union borders and complementing MiCA [93]. The two regulations together also protect EU citizens and bind the operators on the single market at the point where the EU consumer protection rules end, thus filling the gaps that the ESMA warned about ten years earlier, as outlined above.

Importantly, MiCA is not supposed to apply to NFTs; to distinguish between cryptoassets covered by MiCA and financial instruments covered by MiFID II, by 30 December 2024, ESMA will have to issue guidelines on the criteria and conditions for the *qualification of cryptoassets as financial instruments* [94]. MiCA also introduces the concept of *cryptoasset service providers* under EU law. That is, if cryptocurrency or cryptoassets more generally are the subject of a project, or if a tech enterprise provides services related to cryptoassets (custody, purchase/sale of cryptoassets, exchange, reception or transmission of orders, management of portfolio, etc.), such entity qualifies as a service provider covered by MiCA.

The general application date of MiCA and the TFR is 30 December 2024. The cryptoindustry and any tech player that in any way deals with crypto on the EU market now have roughly a year to prepare for full compliance with the new legislation. In general, both regulations aim at guaranteeing a lower risk of being scammed or losing one's cryptos. The regulations also aim at triggering the development of strategic crypto-related projects in the EU, which European tech enterprises and enthusiasts should consider as a

serious and positive message and material support for their efforts. Moreover, the introduction of an *EU passport for cryptoasset service providers*, which will allow them, once authorized, to provide cryptoasset services in all EU jurisdictions, is likely to enhance the possibility to scale-up cryptoprojects at the European level [94].

In sum, in the EU, as far as cryptoassets (including both digital currency and NFTs) are concerned, an in-depth legal and regulatory analysis and constant monitoring are crucial for the covered tech organizations. By the general application date (30 December 2024) of MiCA and the revised TFR, applicants will have limited time in which to implement their requirements, so it is better to prepare all the necessary information, files, and proceedings in advance.

More generally, the bottom line of the finance- and monetary-related regulations that apply to the digital economy and that are relevant to any Web 3-4 enterprise is that knowing and clearly understanding (i) *what* is one's product, content, or service in both monetary and financial terms, (ii) *what* exactly is in one's cryptowallet, and (iii) in *which jurisdiction* one is the taxpayer will define how the entity declares and pays the taxes on its cryptoassets and in which cryptocurrency one would prefer to receive and/or issue one's payments.

8. Conclusions

There is nothing new under the sun. This statement may seem exaggerated, but there is also a good deal of truth to it. Most of the foundations of the legal framework that can be adapted to regulate the new economic space where we all found ourselves almost overnight due to the COVID-19 pandemic —the digital economy— have existed for several decades, and sometimes even centuries, as is the case for some fundamentals of corporate and contract law. This assertion, the main argument of the present article, has been supported by the analysis performed throughout this study. This assertion is especially true with respect to most of the applicable constructs of corporate and contract law, regulatory compliance, ethics, and, to some extent, IP rights.

However, the framework analysed in this paper also tells us, with regard to the specific doctrinal, legislative, and judiciary approaches to the subject matter, that formal law, as a stable pre-existing institution within the actual (centralized) legal systems of advanced capitalist societies, often remains frozen. By contrast, business and, even more so, digital relations advance more rapidly than and sometimes independent of their legal framework. In the context of this article, the relevant digital economic framework evolved into a quite decentralized, and often self-regulated, space in the blind spots of some traditional twentieth and early twenty-first centuries approaches to business organizations, national currencies, national and transnational financial systems, and even freedom of, and on, the internet.

Therefore, on top of the above initial hypothesis supported by the analysis, in the course of this study, I also identified two key developments brought about by the digital transformation. Firstly, this new rather decentralized and increasingly self-regulating digital economic space creates so-called *governance and regulatory gaps*. Secondly, and consequently, some of these gaps are filled rapidly (at times, successfully, at times less so) by a burgeoning *newest legal framework* (national and supranational targeted regulation, legislation, and case law alike) that has been booming since the second decade of the twenty-first century, and especially since the global digital 'leap' caused by the COVID-19 pandemic in the beginning of its third decade.

Regarding the first general finding—the governance and regulatory gaps—the analysis in every section of this paper, while mostly confirming the key argument of the article, uncovered a few such gaps. In particular, these gaps are seen in Section 2, which focuses on corporate and contract law and explains how such online organizations as DAOs may at present not only have a fully de-centralized corporate structure without a central board and/or management, but also exist and do relatively well without any registered legal personhood. There are, of course downsides to such a development: civil and contractual liability bears most of the adverse impact of such entities' existence and operations. Both

research, and legislative and adjudicatory developments regarding this issue are only nascent. There is thus a large avenue for future research and practice on the subject.

In terms of the second general discovery—the proliferating newest legal framework responsible for a 'spotted targeting' of those gaps—another set of tech highlights considered in Section 2 of this article concerned consumer contract law. For example, recall that in Summer 2023, a Canadian court ruled that a 'thumbs-up' emoji represented a contract agreement. This and other similar findings of the section that addressed the conservative fields of corporate and contract law demonstrate that, while we have to adapt the existing rules to the new realities of the digital economy, we also have to thoughtfully create new ones. For those on the receiving end—the tech enterprises—the main message of Section 2 is that, in order to stay sustainable and compliant, a rigorous approach to all relevant details of such constructs as the general terms and conditions of sale, the consumer protection rules in force in a given jurisdiction, and other relevant points analysed in the section are crucial for any digital organization selling or providing any kind of content, goods, or services.

Section 3, which focused on regulatory compliance, also revealed a number of findings stemming from the two strands—i.e., from governance and regulatory gaps and from the newest legal framework aiming to fill those gaps. Online marketplaces and all other kinds of online platforms in any way offering various digital services, goods, and, today, increasingly, content, are, along with DAOs, another typical example of new Web 3-4 'entities'. At present, they may be non-compliant due to unfair or simply dangerous dealings by myriad fund providers, traders, sub-contractors, and even third parties operating on their platforms. They may thus fail to guarantee a safe, transparent, and trustworthy sustainable ecosystem for consumers and the whole economy.

Along with the pre-existing AML, KYC, KYB, due diligence and like regulatory tools outlined in Section 3, the online platforms should thus organize their interface in a way that allows all concerned parties to comply with the corresponding due diligence and information obligations. One of the most recent regulatory developments more typical and adapted to, for instance, services, including financial services that are fully digital, is the EU Digital Services Act that offers a general framework in the subject-matter.

Overall, regarding both general strands—the gaps and filling those gaps—any tech enterprise must take seriously the conception and implementation of its compliance strategy that includes a robust and well-thought risk management. Once it is done, the organization must ensure that its management, operations, and transactions comply with such strategy and pleas, including online pleas.

Section 4 on data showed that the governance and regulatory gaps regarding personal data protection are today increasingly made up by strict regulations around the world. There is also a growing body of case law that makes internet users' personal data governance and protection stricter every day.

At the time of writing, the GDPR—the EU data protection law pre-existing the COVID-related digital revolution—is still the strictest data protection set of rules. Any online company in any way related to the EU single market will have to establish a GDPR register and provide clear information on how exactly it gathers and manages data. Furthermore, Switzerland recently adopted its own data protection law, nFADP, that came into effect on 1 September 2023, and which, in some respects might be even stricter than the GDPR, as the analysis has shown. The actual implementation and enforcement of the newest Swiss data protection law will likely confirm or rebut my above assertion.

If an online entity does not collect personal data, but only collects wallet addresses or transactions, as it is the case of many DAOs and other kinds of FinTech organizations, especially those in any way working with cryptoassets, there are at least two options to stay compliant with relevant data protection law, analysed in the same section of the article.

The last, but definitely not least—and growing—pain point regarding data protection is data's increased gathering, processing, and usage by last-generation AI, including general-purpose AI systems. One of the key issues here is profiling. Profiling by AI today

provides for decisions with legal, socio-economic, psychological, and similarly far-reaching effects on most of the data subject's areas and stages of life, from school to the final years, and even to funerals. Section 4 also addresses these situations, as well as some ways of managing the associated difficulties, especially in Europe.

In the EU, the year 2023 marked several milestones in both legislation and adjudication. As discussed in Section 4, for instance, the AG Opinion in a CJEU case *SCHUFA Holding* on profiling made clear that being subject to such decisions based solely on AI processing is covered by the GDPR, which also grants certain rights to the victims of AI profiling. Moreover, the project of the European AI Act is expected to further the protection of EU citizens' right to file complaints about AI systems and receive explanations of decisions based on high-risk AI systems that significantly impact their fundamental rights. The EU AI Act would also present comprehensive lists of prospectively prohibited AI practices, as well as lists of high-risk AI applications. Under the Act, providers of foundation models on the single market would have several firm obligations outlined in the section, whereas generative AI systems based on such models, such as ChatGPT, would have to comply with a number of strict requirements and establish several safeguards against generating illegal content, including deepfakes. For the moment, these considerations are covered by ethical standards, as addressed in Section 5 of the article. The project of the AI Act also has prospects for far-reaching rules on AI data copyright and other IP-related aspects, the topic analysed in detail in Section 6 of this paper.

On the ethics front (Section 5), the gaps are quite apparent. The online economy, while facilitating our access to virtually any content, good, or service, at present jeopardizes trust and fuels misinformation, polarization, and inequality, as most of the digital tools that today shape our socio-economic relations were developed with few commonly held ethical standards. Here, the new normative development, the prospective EU AI Act, instead of filling the gaps, for the moment merely points to the sheer and urgent need that the technologies that shape our current economy and society be consistent with our shared values and ethical standards.

Regarding AI, today one of the major ethical issues is deepfakes. Section 5 showed that deepfakes can be harmful for myriad areas of our everyday life: education and research, banking and finance, administration of justice, etc. Other highlighted pain points arising from classification AI and generative AI systems naturally include equal access to education, employment, the social system, and the market of goods, services, and content, as well as, more generally, secure and authentic information and, eventually, a safe online space for everyone. At the conceptual level, those issues are reflected in the ethical questions of safety, privacy, and, especially, equality.

As Section 5 showcased, humans are thus classified by AI into new groups that face discrimination. These groups are arbitrary, human incomprehensible, and random because they are defined by incomprehensible and unknown characteristics, and created and deployed by AI in a random manner. These gaps of privacy, safety, and, progressively, equality, are drawing increasing attention from policy-makers and lawyers, who attempt to fill them more formally, especially in the EU, and especially in litigation, as shown by the results of various 2023 CJEU cases.

Regarding the discussion of IP in Section 6, the EU AI Act contains prospects for far-reaching rules on IP-related issues. Until the Act is finalized and becomes effective, the existing rules applying to IP in AI-related business and other concerned elements of the tech world (NFTs, metaverse) are as discussed in Section 6. As outlined, like metaverses themselves, IP law applicable to this issue is still in the nascent, if not embryonic, stage, and more scholarly, regulatory, and policy developments are needed, thus representing rich opportunities for development in these regards.

The AI-related IP analysis was divided into questions on input data for generative AI and questions on its output data. With respect to the input data, it was established that the most relevant IP rights are those pertaining to copyright and database rights. Organizations offering and/or using generative AI should be mindful that when their AI has

been—or might have been—trained on data that is protected by copyright or database rights or both and no exceptions apply, those data must be validly licensed; if they are AI suppliers, they must ensure that actions taken to respect any IP rights concerned are comprehensive and up-to-date; if they are users of such AI, they must seek assurance on this point from the AI supplier.

As to data output by generative AI systems, the two types of IP rights identified as the most relevant are copyright and patents. Regarding the latter, in the EU, for example, inventions generated by AI are not patentable. In 2022, in a related dispute, the European Patent Office decided that a generative AI system cannot be regarded as an inventor. Neither a computer programme that generates an invention without human involvement, nor the owner of such a system, is entitled to a patent. Regarding copyright of the output data, under EU copyright law, works generated purely by AI- or other automated processes lack any form of human input and are, as such, not eligible for copyright protection: AI or any other type of computer programme is copyrightable, but any output they autonomously create is not.

In contrast, for instance, current UK copyright law protects some types of artistic works that are generated entirely by computers, provided that the originality condition is met. Therefore, generative AI may put the copyright originality requirement under pressure across jurisdictions, and this question is an excellent avenue for future research.

Not only does it remain untested whether such works generated by AI would undermine claims to originality, but many of them now also may constitute NFTs—the concept that is radically transforming how IP is understood and regulated and how other legal questions apply to unique, irreplaceable digital content. NFTs are tokenized via blockchain. However, NFTs have no value without the rights attached to the content. Consequently, it is vital for enterprises that are the authors of covered works to know and understand relevant IP rights, to register and protect any intellectual property as soon as possible, and to design IP strategies, including one regarding NFTs.

Notably, many NFTs can be purchased only with cryptocurrency and some NFTs are also traded on cryptocurrency exchanges. Cryptocurrencies are built using the same kind of programming as NFTs are, but that is where the similarity ends. Indeed, cryptos may (or may not) be a kind of money. The last substantive section of this study analysed precisely the monetary and financial aspects of Web 3-4 regulation. Section 7 uncovered more limitations to the applicability and effectiveness of legal and regulatory constructs that pre-existed the digital transformation of the 2020s than all previous sections of the article. It also suggested more options and possibilities.

For instance, the July 2023 judgment of a US District Court in the *Ripple* case, which said that the XRP token at issue was not a security, and especially the ensuing decision by the SEC to appeal the ruling, signalled that today any cryptocurrency except BTC is in the spotlight and under considerable pressure from regulators, both in the US and around the world. The analysis of this important ruling also suggests that any cryptowallet owner must be mindful of, and must constantly monitor the status of, all the tokens in their wallet and whether they are, or are likely in the near future be considered any of the following: currency, 'private money', property, or security. This necessity arises because the method needed to declare and pay one's taxes, as well as the nature of the tokens that one owns, will depend on the applicable law.

The section also showed that even the legal status of the oldest, biggest, and the most expensive crypto, BTC, is subject to change across jurisdictions and over time: while some countries have made it their legal tender, several others have fully or implicitly banned BTC use.

A few jurisdictions use BTC as a kind of exchange token, including Switzerland and the US, and some US states (Colorado) and Swiss cantons (Zug) even accept tax payments in BTC. However, the US central tax authority, the IRS, says that, for tax purposes, BTC and all other private cryptocurrencies are not currency, but property; thus, buying and selling cryptos is taxable under US tax law. Like the US, the UK does not treat private

cryptocurrency as money or currency, which means that anyone in the UK who holds cryptoassets as a personal investment will be taxed on any profits realized on such assets.

In the EU, Germany is one of the most crypto-friendly member states: under current German tax law, BTC and all other cryptos are considered 'private money'; thus, cryptos held longer than one year are not subject to income tax, even if the asset increases in value; individually held crypto is VAT-exempt, and assets held for over a year do not incur a tax liability on earnings.

Supranationally, on the litigation front, the CJEU ruled in 2015 that BTC transactions would be exempt from VAT. On the legislation front, in June 2023, the EU adopted the MiCA and the TFR regulations, which aim to regulate the cryptomarket in the EU and to harmonize the regulatory framework for the cryptoasset market across the Union.

The two regulations complement each other and apply to cryptoassets that are not currently regulated by the existing EU financial services legislation, support innovation and fair competition, delimit the rules for those issuing and trading cryptoassets, and require providers of cryptoasset services to accompany any transfer of cryptoassets with information on the originators and beneficiaries. Together, the two regulations also protect EU citizens there, where the EU consumer protection rules end.

Both regulations aim at ensuring a lower risk of being scammed or losing one's cryptos and aim to trigger the development of strategic crypto-related projects in the EU. TFR also introduces an EU passport for providers of cryptoasset services, allowing them, once authorized, to provide their services in all EU jurisdictions. This passport thus makes more room for scaling-up cryptoprojects at the EU level.

In sum, in the EU, for both cryptocurrency and NFT projects, an in-depth legal and regulatory analysis and constant monitoring are crucial. More generally, the bottom line in cryptoassets regulation is that knowing and clearly understanding (i) the classification of one's product, content, or service (ii) what exactly is in one's cryptowallet, and (iii) in which jurisdiction one is the taxpayer will define how the one declares and pays the taxes on one's cryptoassets, as well as in which cryptocurrency it is preferable to conduct one's transactions.

To conclude, the toolbox proposed in this article (see Figure 1) makes it possible for Web 3-4 entrepreneurs, as well as scholars and practitioners working with legal tech, to identify legal and regulatory red flags and future avenues for attention and development. The toolkit also demonstrates to both the 'giving' (lawyers and policymakers) and the 'receiving' (tech projects) ends of *tech that is liable and sustainable by design* that this field has never been entirely a 'New World' to conquer. Rather, there is 'a method to the madness'. There are defined boundaries, but there is room for a good deal of flexibility and creativity within.

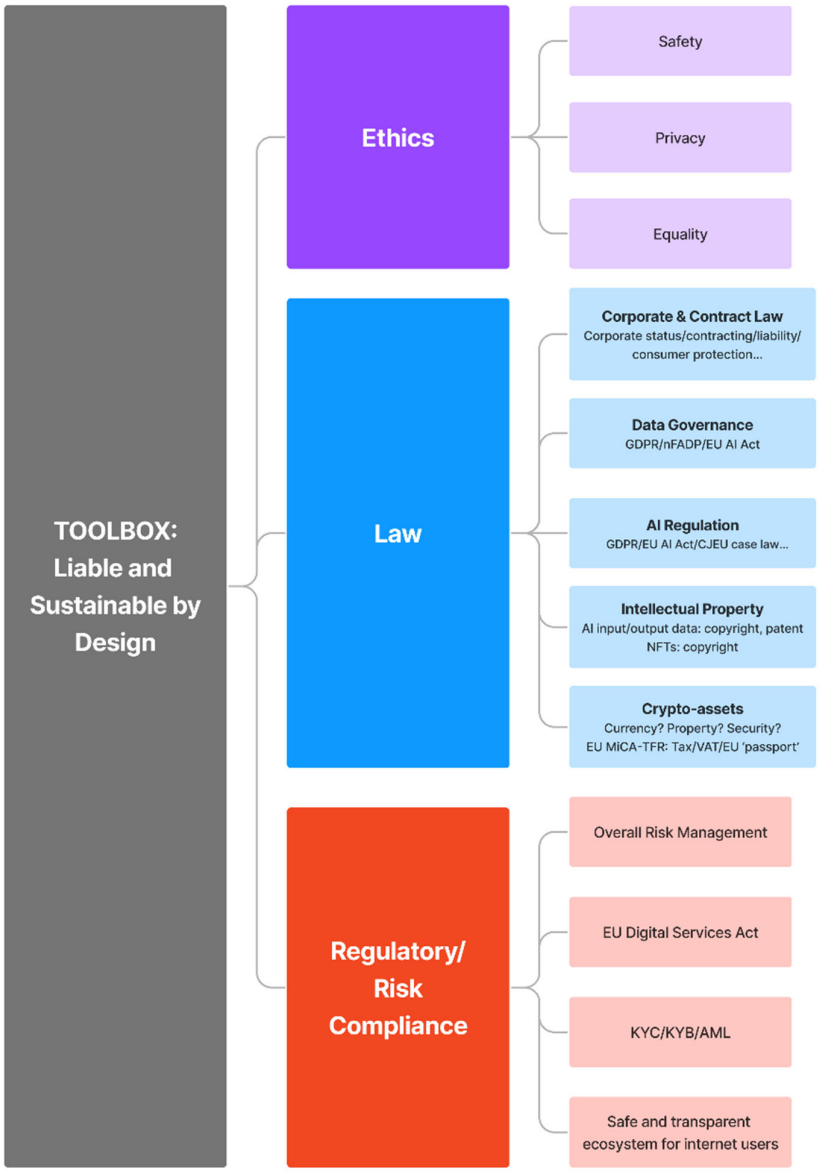

Figure 1. Toolbox for a Regulatory Compliant and Sustainable Tech.

Funding: This research received no external funding.

Informed Consent Statement: I have read and agreed to the published version of the manuscript.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: I am grateful to the five anonymous reviewers.

Conflicts of Interest: The author declares no conflict of interest.

References and Notes

1. Jay Hoofnagle, C.; van der Sloot, B.; Zuiderveen Borgesius, F. The European Union general data protection regulation: What it is and what it means. *Inf. Commun. Technol. Law* **2019**, *28*, 65.
2. Mendoza, I.; Bygrave, L.A. The right not to be subject to automated decisions based on profiling. In *EU Internet Law: Regulation and Enforcement*; Synodinou, T., Jougleux, P., Markou, C., Prastitou, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 77–98.
3. Aseeva, A. *From Corporate Social Responsibility to Corporate Social Liability: A Socio-Legal Study of Corporate Liability in Global Value Chains*; Hart: Oxford, UK, 2021, pp.68-69.

4. Bauman, J.D. Corporations, Law and Policy: Materials and Problems. In *American Casebook*, 7th ed.; West Academic Publishing: Eagan, MN, USA, 2009; pp. 34–35.
5. La Porta, R.; Lopez de Silanes, F.; Shleifer, A. Corporate Ownership Around the World. *J. Financ.* **1998**, *54*, 471+491–496.
6. Bainbridge, S.M. Director Primacy in Corporate Takeovers: Preliminary Reflections. *Stanf. Law Rev.* **2002**, *55*, 791+794.
7. Kraakman, R.; Armour, J.; Davies, P.; Enriques, L.; Hansmann, H.; Hertig, G.; Hopt, K.; Kanda, H.; Pargendler, M.; Ringe, W.-G.; et al. *The Anatomy of Corporate Law: A Comparative and Functional Approach*, 3rd ed.; Oxford University Press: Oxford, UK, 2009, p.28.
8. Berle, A.; Means, G.C. *Modern Corporation and Private Property*; Brace & World: New York, NY, USA; Harcourt: Boston, MA, USA, 1968.
9. Falkon, S. The Story of the DAO—Its History and Consequences. *The Startup*, 24 December 2017. Available online: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee (accessed on 11 November 2023).
10. Ethereum. Available online: https://ethereum.org/en/community/ (accessed on 11 November 2023).
11. Biggs, J. dOrg Founders Have Created the First Limited Liability DAO. *CoinDesk*, 11 June 2019. https://www.coindesk.com/markets/2019/06/11/dorg-founders-have-created-the-first-limited-liability-dao/ (accessed on 11 November 2023).
12. Wright, A. The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges. Stanford Journal of Blockchain Law & Policy. 30 June 2021. Available online: https://stanford-jblp.pubpub.org/pub/rise-of-daos (accessed on 11 November 2023).
13. Hinman, W. Speech Digital Asset Transactions: When Howey Met Gary (Plastic). The US Securities and Exchange Commission (SEC). 14 June 2018. Available online: https://www.sec.gov/news/speech/speech-hinman-061418 (accessed on 11 November 2023).
14. Dubnevych, N. The Best Entities and Countries for DAO Registration in 2023. *Legal Nodes*, 28 June 2023. Available online: https://legalnodes.com/article/choose-a-crypto-friendly-country-for-dao (accessed on 11 November 2023).
15. van Ost, E. Finding a Home for DAOs: A Quick Look into the Most DAO-Friendly Countries. *Peaka*, 23 December 2021. Available online: https://www.peaka.com/blog/web3-dao-friendly-countries/ (accessed on 11 November 2023).
16. Mienert, B. How can a decentralized autonomous organization (DAO) be legally structured. *LRZ Legal*, 24 November 2021. Available online: https://lrz.legal/de/lrz/how-can-a-decentralized-autonomous-organization-dao-be-legally-structured (accessed on 11 November 2023).
17. Based on Aseeva, A. Global trade governance and informal voluntary standards: The socionormative analysis of legitimacy of the ISO. In *Multilateralism in Global Governance: Formal and Informal Institutions;* Tutumlu, A., Gungor, G., Eds.; Peter Lang: Oxford, UK, 2016; pp. 71+74.
18. Directive of the European Parliament and of the Council 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance. *Off. J. Eur. Union* **2011**, *L304*, 64–88.
19. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Off. J. Eur. Communities* **1993**, *L95*, 29–34.
20. European Commission; Directorate-General for Health and Consumers; SANCO. Green Paper on the Review of the Consumer Acquis; COM/2006/0744 Final. 2007. Available online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0744:FIN:en:PDF (accessed on 11 November 2023).
21. European Commission. E-Commerce Directive. Available online: https://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive (accessed on 11 November 2023).
22. European Commission. The Digital Services Act Package. Available online: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (accessed on 11 November 2023).
23. Baudouin, J.L. *Les Obligations*; Yvon Blais: Cowansville, QC, Canada, 1989; p. 109.
24. France, French Consumer Code, Revised Version, 2014, Articles L121-16, L-121-20-2, L121-20-12. Available online: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069565/LEGISCTA000006161820/#LEGISCTA000006161820 (accessed on 13 December 2023).
25. ProCDInc v Zeidenberg, 86 F 3d 1447 (Seventh Circ 1996). Available online: https://casetext.com/case/procd-incorporated-v-zeidenberg (accessed on 11 November 2023).
26. Hill v Gateway, 105 F 3d 1147 (Seventh Circ 1997). Available online: https://casetext.com/case/hill-v-gateway-2000-inc? (accessed on 11 November 2023).
27. South West Terminal Ltd. v Achter Land, 2023 SKKB 116 (CanLII) [South West Terminal]. Available online: https://images.assettype.com/barandbench/2023-07/17ed50ce-4edd-472a-be49-91d1c5e6b402/South_West_Terminal_Ltd_v_Achter_Land___Cattle_Ltd.pdf (accessed on 11 November 2023).
28. European Commission. Questions and Answers: Digital Services Act. Available online: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (accessed on 13 December 2023).
29. In the EU, It is the GDPR that applies in all member-states, already referred to above in this article. In Switzerland, the new FEDERAL Act on data protection (nFADP) came into effect on 1 September 2023. See Swiss Federal Council, new federal act on data protection (nFADP). Swiss federal council. New federal act on data protection (nFADP). Available online: https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html (accessed on 13 December 2023).
30. In the US, there is no comprehensive national privacy law, but a number of largely sector-specific data privacy and Data security laws at the federal level, as well as many more privacy laws at the state (and local) level. In recent years, beginning with california, states have begun to introduce their own comprehensive privacy laws, and other states are expected to follow and enact

their own comprehensive state privacy laws. Although a bipartisan draft bill (American data privacy and protection act) was introduced in 2022, several senators were in opposition of the bill, and comprehensive privacy law on the federal level is not expected to pass any time soon. DLA Piper. Data Protection Laws of the World. Available online: https://www.dlapiperdataprotection.com/index.html?t=law&c=US#:~:text=Under%20the%20comprehensive%20US%20state,information%20for%20targeted%20advertising%20purposes (accessed on 13 December 2023).

31. Importantly, on 9 August 2023, india passed its long-awaited data protection bill. Since india is the world's fifth largest economy and an important global tech and outsourcing hub, their new data bill, which is as extraterritorial as the gdpr, will have a broad implication for the data governance inside and outside india. Prs India. The digital personal data protection bill. 2023. Available online: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (accessed on 13 December 2023).
32. Pistor, K. Rule by Data: The End of Markets? *Law Contemp. Probs.* **2020**, *83*, 101.
33. CJEU. Judgment of the Court in Case C-252/21. Meta Platforms and Others (General Terms of Use of a Social Network). Available online: https://curia.europa.eu/juris/liste.jsf?num=C-252/21 (accessed on 11 November 2023).
34. CJEU. Norra Stockholm Bygg, C-268/2 (2 March 2023) [Norra Stockholm]. Available online: https://curia.europa.eu/juris/liste.jsf?language=fr&td=ALL&num=C-268/21 (accessed on 11 November 2023).
35. AG ĆAPETA. Opinion in the CJEU Case Norra Stockholm Bygg, C-268/2 (6 October 2022). Available online: https://curia.europa.eu/juris/document/document.jsf?text=&docid=266841&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=7748458 (accessed on 11 November 2023).
36. AG PIKAMÄE. Opinion in the CJEU Case SCHUFA Holding, C-634/21, (16 March 2023) [SCHUFA Holding]. Available online: https://curia.europa.eu/juris/documents.jsf?num=C-634/21 (accessed on 11 November 2023).
37. Aseeva, A. 'Good AI augments humans, not vice versa' they say. Does it augment human rights?' An updated english-language version of a note for business and human rights, the United Nations global compact network poland report 2022. Available online: https://www.legal-design-garden.com/post/good-ai-augments-humans-not-viceversa-they-say (accessed on 15 December 2023).
38. Korff, D. *Comments on Selected Topics in the Draft EU Data Protection Regulation*; London Metropolitan University: London, UK, 2012. Available online: http://ssrn.com/abstract=2150145 (accessed on 15 December 2023).
39. De Hert, P.; Gutwirth, S. Regulating profiling in a democratic constitutional state. In *Profiling the European Citizen*; Hildebrandt, M., Gutwirth, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2008.
40. Wachter, S.; Mittelstadt, B.; Floridi, L. Why a Right to Explanation of Automated Decision-Making does Not Exist in the General Data Protection Regulation. *Int. Data Priv. Law* **2017**, *7*, 76.
41. Zuiderveen Borgesius, F.J. *Improving Privacy Protection in the Area of Behavioural Targeting*; Kluwer Law International: The Hague, The Netherlands, 2015; pp. 283–93.
42. Edwards, L.; Veale, M. Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for. *Duke Law Technol. Rev.* **2017**, *16*, 18.
43. European Parliament. MEPs Ready to Negotiate First-Ever Rules for Safe and Transparent AI. 14 June 2023. Available online: https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-forsafe-and-transparent-ai (accessed on 15 December 2023).
44. European Parliament. European Parliament. Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI. Available online: https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai (accessed on 15 December 2023).
45. European Parliament. General-Purpose Artificial Intelligence. 1 March 2023. Available online: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf (accessed on 15 December 2023).
46. Generative AI is a form of machine learning that has been trained on vast quantities of data and has mapped patterns across the data, enabling It to generate similar data that is often very difficult to distinguish from content created by a human. Generative AI is able to create content in response to an input prompt. This may involve generating answers in text form in response to a question, or an image or piece of video in response to a text prompt. Osborne clarke. Generative AI: Is its output protectable by intellectual property rights? 8 June 2023. Available online: https://www.osborneclarke.com/insights/generative-ai-its-output-protectable-intellectual-property-rights (accessed on 15 December 2023).
47. Aseeva, A. How (and Why) to Balance PRIVACY Rights and PUBLIC Policy in Digital Economy: AI and Your Data. Legal Design GARDEN Blog, 13 April 2023. Available online: https://www.legal-design-garden.com/post/how-and-why-to-balance-privacy-rights-and-public-policy-in-digital-economy-ai-and-your-data (accessed on 17 December 2023).
48. Wachter, S. The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law. *Tulane Law Rev.* **2022**, *97*, 149.
49. Gerke, S.; Minssen, T.; Cohen, G. Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial Intelligence in Healthcare*; Academic Press: Cambridge, MA, USA, 2020; pp. 295–336.
50. Gillis, T.B. False Dreams of Algorithmic Fairness: The Case of Credit Pricing. *SSRN J.* 2020. Available online: https://www.ssrn.com/abstract=3571266 (accessed on 17 December 2023).
51. Hildebrandt, M. Defining Profiling: A New Type of Knowledge? In *Profiling the European Citizen*; Hildebrandt, M., Gutwirth, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 17–45.
52. Abbott, F.M. Intellectual Property, International Protection. In *Max Planck Encyclopedia of Public International Law*; Oxford University Press: Oxford, UK, 2014.

53. IP law applicable to metaverse is still under construction, but the excesses in the field have already shown how urgent it is to take a clear regulatory and ethical position on the subject-matter. For IP essentials for metaverse, See, e.g., WIPO. The metaverse, NFTs and IP Rights: To regulate or not to regulate? *WIPO Magazine*, June 2022. Available online: https://www.wipo.int/wipo_magazine/en/2022/02/article_0002.html (accessed on 17 December 2023).
54. Osbornee, C. Generative AI: How Sourcing Data for Training AI Tests UK and EU Intellectual Property Rules. 20 April 2023. Available online: https://www.osborneclarke.com/insights/generative-ai-how-sourcing-data-training-ai-tests-uk-and-eu-intellectual-property-rules (accessed on 17 December 2023).
55. The UK Copyright and Rights in Databases Regulations 1997. Available online: https://www.legislation.gov.uk/uksi/1997/3032/contents (accessed on 17 December 2023).
56. EPO. Boards of Appeal, Oral Proceedings, J0008/20-3.1.01 (DABUS Case). Available online: https://www.epo.org/en/boards-of-appeal/decisions/j200008eu1 (accessed on 17 December 2023).
57. EPO. European Patent Convention: Guidelines for Examination; Part G, Chapter II, 3.3.1 Artificial Intelligence and Machine Learning. Available online: https://new.epo.org/en/legal/guidelines-epc/2023/g_ii_3_3_1.html (accessed on 17 December 2023).
58. Bently, L.; Sherman, B.; Gangjee, D.; Johnson, P. *Intellectual Property Law*; Bently, L., Sherman, B., Gangjee, D., Johnson, P., Eds.; Oxford University Press: Oxford, UK, 2018, pp.126-127.
59. Guadamuz, A. Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works. *Intellect. Prop. Q.* **2017**, *2*, 169.
60. Bonadio, E., McDonagh, L. Artificial Intelligence as Producer and Consumer of Copyright Works: Evaluating the Consequences of Algorithmic Creativity. *Intellect. Prop. Q.* **2020**, *20*, 112.
61. In the UK, for instance, even works that are computer-generated (and which have no human author) will be protected by copyright. Ownership of the copyright belongs to the person who has made the necessary 'arrangements' for the work's creation. UK Copyright, designs, and patents act 1988, Section 9(3). Available online: https://www.legislation.gov.uk/ukpga/1988/48/contents (accessed on 17 December 2023).
62. ECR, Infopaq International A/S v Danske Dagblades Forening [2009] ECR I-6569. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0005 (accessed on 17 December 2023).
63. Note that purely computer-produced output might be protected by related or neighbouring rights, such as sound recording rights (that is, phonographic rights), rights of film producers, and so on. for example, phonographic rights include rights of reproduction, distribution and communication to the public. Provided that the definition of a 'phonogramme' is met by such an output, then phonographic rights might be available. Where recordings are generated by ai, the right will be allocated to the producer of the phonogram. This will most likely be the user of the AI software, as opposed to the AI developer, as the user will trigger the act of fixation (a necessary requirement to meet the definition of phonogramme) by deploying the AI system. See, Generally, World Intellectual Property Organization, WIPO Performances and Phonograms Treaty, TRT/WPPT/001. Available online: https://www.wipo.int/wipolex/en/text/295477 (accessed on 17 December 2023).
64. Arnold, R.; Bently, L.; Derclaye, E.; Dinwoodie, G. The Legal Consequences of Brexit Through the Lens of IP Law. *Judicature* **2017**, *101*, 65.
65. Coin Telegraph. Fungible vs. Nonfungible Tokens: What Is the Difference? Available online: https://cointelegraph.com/learn/fungible-vs-nonfungible-tokens-what-is-the-difference (accessed on 18 December 2023).
66. Ethereum. Improvement Proposals (EIPS), ERC-721: NonFungible Token Standard. Available online: https://eips.ethereum.org/EIPS/eip-721 (accessed on 18 December 2023).
67. See, e.g., Binance, Which, at the Time of Writing, Is the Biggest World Cryptocurrency Exchange. Binance. Available online: https://www.binance.com/en (accessed on 18 December 2023).
68. The most iconic meme in internet history, at the time of writing, the doge, is fractionalized and available for anyone to own through buying its piece, which is an NFT. CoinMarketCap. About the doge NFT. Available online: https://coinmarketcap.com/currencies/the-doge-nft/ (accessed on 18 December 2023).
69. Coin Telegraph. What Is Cryptocurrency? A Beginner's Guide to Digital Currency. Available online: https://cointelegraph.com/learn/what-is-a-cryptocurrency-a-beginners-guide-to-digital-money (accessed on 18 December 2023).
70. Coin Telegraph. Tokens News. Available online: https://cointelegraph.com/tags/tokens (accessed on 18 December 2023).
71. Strange, S. *What Theory? The Theory in Mad Money*; CSGR Working Paper No. 18/98, 1 December 1998; Centre for the Study of Globalisation and Regionalisation (CSGR), University of Warwick: Coventry, UK, 1998.
72. The Digital Dollar Project. Available online: https://digitaldollarproject.org/ (accessed on 18 December 2023).
73. Fabrichnaya, E. Russia to Widen Scope of Digital Rouble Testing from Aug. 15—Central Bank. *Reuters*, 9 August 2023. Available online: https://www.reuters.com/markets/currencies/russia-widen-scope-digital-rouble-testing-aug-15-central-bank-2023-08-09/ (accessed on 18 December 2023).
74. Rooney, K. SEC Chief Says Agency Won't Change Securities Laws to Cater to Cryptocurrencies. *CNBC*, 6 June 2023. Available online: https://www.cnbc.com/amp/2018/06/06/sec-chairman-clayton-says-agency-wont-change-definition-of-a-security.html (accessed on 18 December 2023).
75. SEC. SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering. 22 December 2020. Available online: https://www.sec.gov/news/press-release/2020-338 (accessed on 18 December 2023).
76. SEC v. Ripple Labs; et al., 20-cv-10832 (S.D.N.Y) [Ripple]. Available online: https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf (accessed on 18 December 2023).

77. Mascianica, S.; Magee, J.B.; McCarron Turner, C. SEC v. Ripple: When a Security Is Not a Security. Summary Judgment Battle Results in Split Decision, Blow to SEC Enforcement. Holland & Knight, 20 July 2023. Available online: https://www.hklaw.com/en/insights/publications/2023/07/sec-v-ripple-when-a-security-is-not-a-security (accessed on 18 December 2023).
78. Versprille, A. SEC Signals Appeal to Crypto Ripple Ruling in Terra Response. *Bloomsberg Law*, 22 July 2023. Available online: https://news.bloomberglaw.com/securities-law/sec-signals-appeal-to-crypto-ripple-ruling-in-terra-response (accessed on 18 December 2023).
79. Gek, T.P. High Court Rules Crypto Asset Holder Has Legally Enforceable Property Right in Landmark Decision. *The Straits Times*, 2023. Available online: https://www.straitstimes.com/business/companies-markets/high-court-rules-crypto-asset-holder-has-legally-enforceable-property-right-in-landmark-decision (accessed on 18 December 2023).
80. Renteria, N.; Wilson, T.; Strohecker, K. In a World First, El Salvador Makes Bitcoin Legal Tender. *Reuters*, 9 June 2021. Available online: https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/ (accessed on 18 December 2023).
81. Note that in 2023, the country reversed its decision. Central banking newsdesk. CAR to drop crypto as legal tender. *Central Banking*, 27 March 2023. Available online: https://www.centralbanking.com/central-banks/currency/digital-currencies/7956294/car-to-drop-crypto-as-legal-tender (accessed on 18 December 2023).
82. United States Library of Congress. Regulation of Cryptocurrency Around the World: November 2021 Update. Available online: https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf (accessed on 18 December 2023).
83. Financial Review. ACCC Investigating Why Banks Are Closing Bitcoin Companies' Accounts. *Financial Review*, 19 October 2015. Available online: http://www.afr.com/technology/accc-investigating-why-banks-are-closing-bitcoin-companies-accounts-20151018-gkc5iv (accessed on 18 December 2023).
84. The Guardian; Australian Associated Press. Bitcoin Firms Dumped by National Australia Bank as Too Risky. *The Guardian*, 10 April 2014. Available online: https://www.theguardian.com/world/2014/apr/10/bitcoin-dumped-by-national-australia-bank-as-too-risky (accessed on 18 December 2023).
85. The Denver Post. Colorado Accepts Cryptocurrency to Pay Taxes, Moving the State Tech Forward. *The Denver Post*, 21 September 2022. Available online: https://www.denverpost.com/2022/09/21/colorado-accepts-cryptocurrency-taxes/ (accessed on 18 December 2023).
86. Canton of Zug. Canton Zug to Accept Cryptocurrencies for Tax Payment Beginning in 2021. 3 September 2020. Available online: https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/kanton-zug-akzeptiert-ab-2021-kryptowaehrungen-fuer-steuerzahlungen/medienmitteilungen/press-release-of-september-3rd-2020-english-version/download (accessed on 18 December 2023).
87. Coin Telegraph. A Beginner's Guide to Filing Cryptocurrency Taxes in the US, UK and Germany. Available online: https://cointelegraph.com/learn/filing-cryptocurrency-taxes-in-the-us-uk-and-germany (accessed on 18 December 2023).
88. Clinch, M. Bitcoin Now Tax-Free in Europe after Court Ruling. *CNBC*, 22 October 2015. Available online: https://www.cnbc.com/2015/10/22/bitcoin-now-tax-free-in-europe-after-court-ruling.html (accessed on 18 December 2023).
89. European Banking Authority (EBA). Warning to Consumers on Virtual Currencies; EBA/WRG/2013/01. 12 December 2013. Available online: https://web.archive.org/web/20131228224508/http://www.eba.europa.eu/documents/10180/16136/EBA+Warning+on+Virtual+Currencies.pdf (accessed on 18 December 2023).
90. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). *Off. J. Eur. Union* **2023**, *L150*, 40–205.
91. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain Crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance). *Off. J. Eur. Union* **2023**, *L150*, 1–39.
92. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast). *Off. J. Eur. Union* **2014**, *L173*, 349–496.
93. European Securities and Markets Authority (ESMA). Digital Finance and Innovation: Markets in Crypto-Assets Regulation (MiCA). Available online: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica#:~:text=The%20Markets%20in%20Crypto%2DAssets,by%20existing%20financial%20services%20legislation (accessed on 18 December 2023).
94. Bartlam, M.; Berger, P.E.; Boeve, M.; Kalokyris, N. MiCA & TFR: The Two New Pillars of the EU Crypto-Assets Regulatory Framework. *DLA Piper*, 20 June 2023. Available online: https://www.dlapiper.com/en/insights/publications/2023/06/mica-tfr-the-two-new-pillars-of-the-eu-cryptoassets-regulatory-framework (accessed on 18 December 2023).