Some implications of the new global digital economy for financial regulation and supervision

José Carlos Laguna de Paz

Accepted: 23 January 2022 / Published online: 18 February 2022
© The Author(s), under exclusive licence to Springer Nature Limited 2022

Abstract
The digital economy is leading to substantial changes in the financial sector. Not surprisingly, it raises a number of sensitive legal issues. (1) New technologies and big data are expected to increase efficiency in the financial sector. But some limits need to be drawn in order to protect the fundamental rights at stake, such as privacy and non-discrimination. (2) The application of the so called supervisory technology (SupTech) can improve financial supervision, but it does not seem to alter its legal foundations. (3) We have to consider the role that big techs might play in the financial system and whether they should be subject to a tailor made regulation. (4) Digital currencies take us to the basics of what money is and to wonder what the role of the State is in relation to it. (5) Finally, we have to consider the implications that the creation of an official digital currency could have for the financial system.

Keywords Financial sector · Regulation and supervision · Digital economy · Digital euro · Artificial intelligence · Cryptocurrencies · SupTech · CBDS

Introduction
The new global digital economy may trigger a real disruption in the financial sector, with new players, services and ways of doing business. The extent to which it will occur is still unknown, but there are reasons to think that we are at the beginning of the digital revolution in the financial sector.¹ To give just a few examples, in June 2019 the financial world was shocked by Facebook’s announcement to create a cryptocurrency (Libra now called Diem). It is worth noting that a chat application as popular as WhatsApp (Facebook) is already providing payment services in some parts of the world, enabling users to make transactions to their contact list. It is also very significant that in the US some states have approved legislation allowing cryptocurrency companies to obtain a bank license, subject to specific conditions.² We have also just witnessed the first major cryptocurrency exchange to go public in the US (Coinbase). The mayor of Miami has even proposed to pay municipal workers in Bitcoin, in efforts to make the city a centre for tech industry innovation.

We can assume that this overall process is very likely to bring clear benefits in terms of competition, innovation and efficiency. However, at the same time, we cannot overlook the serious risks that the global digital economy involves for the financial system. On the one hand, the digital economy could lead to a very concentrated financial market, dominated by a handful of big techs, which could replace commercial banks in the provision of financial services (“And yet a world without banks is also visible on the horizon”).³ On the other hand, decentralised finance (DeFi) is a quickly rising phenomenon seeking to eliminate intermediaries in financial transactions, which would be replaced with

¹ Wuermeling, J. (2021) Combining stability and innovation—the Bundesbank and fintech players in the digital financial ecosystem. BIS [https://www.bis.org/review/r210129a.htm (accessed 29 January 2021)].
² Emamian, M. (2021) The Cowboy State Tames Bitcoin’s Regulatory Wild West. The Regulatory Review, 7 April [https://www.theregulatoryreview.org/2021/04/07/emamian-cowboy-state-tames-bitcoins-regulatory-wild-west/ (accessed 7 April 2021)].
³ The Economist (2021) A future with fewer banks, 8 May [https://www.economist.com/special-report/2021/05/08/a-future-with-fewer-banks (accessed 6 May 2021)].
software protocols. In both scenarios, financial regulation and supervision would become extremely difficult. Monetary policy could also blow away from state control and even financial sovereignty would be under threat.

More likely, things will not go that far. Probably we will be in a situation halfway between where we stand now and the described world. Any case, regulation should aim to anticipate the problems. That is to say that we might need to make some adjustments to the current legal framework to respond to the new challenges. Not surprisingly, there is no certainty in this respect, but a lively debate among regulators around the world about what should be done. Some countries have passed some pieces of legislation to address certain issues or have adopted regulatory sandboxes (UK, the Netherlands, Denmark, Spain and several states in the USA).

The European Commission has proposed a Digital Financial Strategy, which aims to provide a comprehensive response to the new challenges. Firstly, the proposal is intended to eliminate fragmentation in the digital single market, enabling cross-border financial services. This may need changes in the regulatory framework for anti-money laundering, counter-terrorism financing, electronic identification and trust services for electronic transactions. Secondly, the European Commission intends to adapt the EU regulatory framework to facilitate digital innovation through distributed ledger technology (crypto-asset regulation), artificial intelligence and cloud computing. Thirdly, the proposal is also intended to facilitate access to data and data sharing, which would improve services, while complying with data protection and competition rules. Fourthly, the strategy aims to address the risks associated with the digital transformation of the financial sector in order to safeguard financial stability, consumer protection, market integrity, fair competition and security.

In this context, international cooperation will be critical for the effectiveness of this policy, due to the cross-border nature of digital financial services.

In this paper, we are going to point out some implications that the new global digital economy has for the regulation and supervision of the financial sector, as they are seen today. In particular, we will focus on six topics, which are closely related. (1) Big data is at the heart of the new economy, which raises the question of legal protection in relation to the processing of personal data (point II). (2) Financial business is expected to rely increasingly on artificial intelligence (AI). In this regard, we have to wonder whether there should be limits to the use of personal data to make business decisions (point III). (3) Machine learning and AI are also being applied for financial regulation and supervision, which is called supervisory technology (SupTech) (point IV). (4) As we have advanced, digital revolution is bringing new operators to the financial scene, which might become major players. In other words, we have to consider the role that big techs are likely to play in the financial system (point V). (5) Digital currencies lead us to question what money is and what the role of the state is in relation to it (point VI). (6) Finally, we need to address the possible creation of Central Bank Digital Currencies (CBDCs) and their implications for the financial system (point VII).

Personal data protection

New technologies are rapidly transforming the financial sector. In some countries robots are already performing banking tasks, such as customer contact and processing of loan applications. The importance of big data, machine learning and AI in the financial sector is expected to grow. All this can lead to a more efficient financial sector, but it also raises a number of questions. Among them, the protection of...
personal data is a matter of serious concern. The financial sector is a big source of data, which can easily be collected and treated by operators. We cannot exclude that the interest of large technology companies in providing payment services, at least in part, is data collection.

There is no equal sensitivity and degree of protection in relation to personal data in the different parts of the world. Significantly, there are important differences between the EU and the US in this respect. Nevertheless, the stricter EU legislation has exercised a wide influence in the world. To some extent, the EU’s General Data Protection Regulation has become the global standard.

In the EU, there are limits to the processing of personal data resulting from the right of data protection, which is a fundamental right recognised at national level and by Article 8(1) of the Charter of Fundamental Rights of the European Union and by Article 16(1) of the Treaty on the Functioning of the European Union. In short, data are to be collected for specified, explicit and legitimate purposes and processed in a transparent manner. The point is that although having these guarantees the European legislation is very much based on consent given to the processing of personal data. In this regard, we should wonder whether this is actually sufficient to effectively protect personal data. Personal data may be the price for receiving services free of charge. However, every day we are giving our consent to the processing of our data without having had time to read on what we have agreed to. At least, we should improve the citizen’s ability to make more informed decisions. Moreover, we could go a step further. It might be appropriate that legislation would prohibit more strictly the processing of personal data, as currently happens with medical data. Arguably, a rule could be established that payment intermediaries and commercial banks would not have access to the data, which would be encrypted. Access would only be granted to resolve disputed charges.

In a global economy, legislation has to ensure that data are not transmitted to third-countries if they do not have equivalent protection. According to the EU legislation, the transmission of data to third-countries or international organisations would require: (1) the country has been declared by a European Commission decision as having equivalent protection (‘adequacy decision’), which has to be read in the light of the Charter of Fundamental Rights of the EU; (2) the adoption of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals; (3) or the presence of a number of derogations (informed consent).

The Court of Justice of the European Union has interpreted this right in a strict manner. In this sense, data protection applies no matter whether data transferred are to be processed by the authorities of the third country for the purposes of public security, defence and State security. Thus, on the occasion of data concerning a European user that Facebook Ireland (subsidiary) had transmitted to Facebook Inc. in the US, the Court found that the protection provided by this country was not sufficient, since data were likely to be consulted and processed by the US authorities in a manner incompatible with the right, as protected by the Charter. In addition, it was found that EU citizens do not have the same remedies as US citizens in respect of the processing of personal data by the US authorities, since the Fourth Amendment to the US Constitution does not apply to them.

**Do fundamental rights set limits to business decisions?**

Having big data at their disposal, financial business is expected to be increasingly based on AI. Computers can help financial players make more secure investment decisions, better control the risks associated to their financial services or improve fraud control (for instance, to detect odd behaviour in the use of credit cards). All this can bring benefits for financial players, as well as for their customers and as a result for the financial stability. However, some points need to be considered more carefully.

Decisions to grant a loan are made on a personal basis. However, in the near future such decisions could be made automatically on the basis of our own personal characteristics, which would result from thousands of pieces of information (time of day purchases, browsing histories, etc.). Commercial banks are private companies that seek to make a profit. By doing so, they also contribute to preserving financial stability. In addition, a more informed analysis may lead to a loan being granted to someone who

---

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

13 The Economist (2021) The EU wants to become the world’s super-regulator in AI, 24 April [https://www.economist.com/europe/2021/04/24/the-eu-wants-to-become-the-worlds-super-regulator-in-ai (accessed 26 April 2021)].

14 Article 6.1.a) of Regulation (EU) 2016/679.

15 Carstens, A. (2021) Data, technology and policy coordination BIS, 14 September, p. 2 [https://www.bis.org/speeches/sp191114.htm (last visited: 20.4.2021)].

16 Articles 44–50 of Regulation (EU) 2016/679.

17 Case C-311/18, Data Protection Commissioner, EU:C:2020:559.

18 Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, EU:C:2020:559.

19 Case C-362/14, Schrems II, EU:C:2015:650.
would otherwise had been denied. However, if personal life could be scrutinised at detail privacy would disappear. On the other hand, it raises concerns about possible bias, discrimination or unfairness towards consumers. Computer codes are not driven by subjective motives, but are written by humans who may be driven by subjective motives. In the new tech-driven finance, the ability to determine what exactly the code does, and what it does not do, is a source of potentially immense power. Moreover, this power is often hidden from the vast majority of market participants who have no means of evaluating the technical qualities of the algorithm. Data management could allow financial institutions to introduce price discrimination practices, that is charging more for the same service to customers depending on their willingness to pay.

The issue is to what extent it is fair to use gender, age, likes or consume patterns to predict which customers would have a higher likelihood of default. This question has no easy answer.

We can accept that some limits directly result from the fundamental rights at stake. In this regard, the use of AI could put in danger the right to human dignity (Article 1 of the Charter), the respect for private life and protection of personal data (Articles 7 and 8 of the Charter), the right to non-discrimination (Article 21 of the Charter) and the right of equality between women and men (Article 23 of the Charter).

However, the extent to which fundamental rights apply in relations between citizens is very controversial. In fact, price discrimination is usual in the provision of services. The price charged for medical or life insurance depends on very personal factors. But, for example, should airlines be able to charge more for people who weigh more? So where do we draw the line? Would that such tailor-made business practices not lead to an unbearable degree of lack of solidarity which is detrimental to society itself? Many are worried about the risk of algorithms ending up in discrimination against certain groups of people.

As we have said, where appropriate, it would be a task for legislators to set limits on the commercial freedom of financial actors, who would otherwise be able to make their decisions as they see fit. It is not an easy task to draw the line between what should be permissible and what should not. Significantly, the proposed EU legislation prohibit only for public authorities discriminations based on the use of AI for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics (Article 5.1.c). But also significantly AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score in relation to essential private services are classified as high-risk (Annex III, 5.b).

In this regard, we might ask whether self-regulation would be a way to address these issues. For instance, Facebook has established an “oversight board”, composed of independent members, to which big tech’s decisions can be appealed (account cancelation). However, it is very doubtful that self-regulation could be appropriate for an effective protection of privacy.

Taking all this into account, it possibly would be better to protect personal data in more effective way than just giving the individuals the right to consent to their processing.

Any case, no matter whether the decision is made by a human being or a machine, the financial player takes full responsibility for it. At this regard, it seems appropriate the proposed EU legislation requiring transparency and traceability of the AI systems, in order to ensure effective redress for affected persons.

New technologies applied to financial supervision

Digital finance makes supervision more challenging. The number of actors and financial products is mushrooming. Financial transactions take place very quickly. Regulators and supervisors need to understand the risks associated to the algorithms applied by the financial players. In the digital economy, data collection and analysis are also essential for central banks to identify risks, design policy and take action in a timely and targeted manner.

---

20 Kalifa Review of UK Fintech (2021), 26 February, p. 27 [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971370/KalifaReviewofUKFintech.pdf (accessed 24 May 2021)].

21 Omarova, S. T. (2020) Technology v Technocracy: Fintech as a Regulatory Challenge. Journal of Financial Regulation, 6, p. 91.

22 Carstens (2021), p. 2.

23 The Economist (2021) The EU wants to become the world’s super-regulator in AI, 24 April [https://www.economist.com/europe/2021/04/24/the-eu-wants-to-become-the-worlds-super-regulator-in-ai (accessed 26 April 2021)].

24 Baldwin, R., Cave, M., Lodge, M. (2012) Understanding Regulation. Theory, Strategy and Practice, Second Edition. Oxford: Oxford University Press, pp. 137–164.

25 The Economist (2021) Will Facebook’s “Supreme Court” reinstate Donald Trump’s account?, 17 April [https://www.economist.com/united-states/2021/04/15/will-facebook-s-supreme-court-reinstate-donald-trumps-account (accessed 19 April 2021)].

26 COM (2021) 206 final, 11.

27 Omarova (2020), p. 100.

28 Ramsden, D. (2021) The Bank of England and Fintech: Public Support for Private Innovation, 21 April, p. 4 [https://www.bis.org/review/r210421c.pdf (last visited: 21.4.2021)].
All this explains that central banks and supervisory authorities are increasingly using new technologies to exercise their regulatory and supervisory competences.\textsuperscript{29} There can be little doubt that the so-called supervisory technology (SupTech)\textsuperscript{30} can improve supervision and enforcement by authorities, reducing the scope for human error. However, the overreliance on the use of these new methods can be also a risk. Not to mention the risks related to cyber-attacks. In any case, the point is to what extent SupTech can have legal implications.

The mere use of new technological tools -including machine learning and AI- do not seem to alter the legal foundations of financial supervision. We should not allow decisions to be made by machines. Automated actions can prepare or support administrative decisions, but are not administrative decisions. In other words, supervision will be made by a human being with the help of a machine. In this sense, we may be well expecting more statistical approaches to supervision where decisions will be taken based on empirical-based probability assumptions rather than case-by-case scrutiny of files.\textsuperscript{31} But at the end of the day, we will be facing decisions made by the central bank or by the competent administrative authority, no matter whether they rely on a technical analysis made by a computer. Consequently, decisions need to contain a statement of reasons, which is an essential requirement to protect the rights at stake.

Provision of financial services by big techs

Big techs have entered the financial sector, in particular by offering payment services. These services are provided in cooperation with the traditional financial players or competing with them. The role of big techs is even greater in developing countries, where they might replace weaker commercial banks by offering a varied range of services (credits, insurance, crowdfunding, etc.).

There is no doubt that big techs have a potential for innovation and efficiency, but when providing financial services, they need to be subject to a proper regulation and supervision. In fact, big techs have to comply with the relevant legislation and need a prior licence for providing banking and payment services, managing assets or offering insurance services. So far only very few jurisdictions have approved specific licence requirements for digital banks.\textsuperscript{32} The issue is whether big techs should be subject to a tailor-made regulation, aimed to ensure financial stability, a level playing field among operators and consumer protection.

Big techs do not currently represent a threat to the banking system, but they could quickly become systematically important.\textsuperscript{33} Big techs do not just provide services, but they have at the very core of their business a technological platform which is used for an ever-increasing number of users to reach their customers. The undeniable usefulness of technological platforms, which highly reduce transaction costs, is creating a significant degree of dependence for both business and end users. It allows big techs to keep for themselves a large portion of the rents extracted from participants to the multisided markets intermediated by platforms.\textsuperscript{34} At the same time, these platforms are hardly contestable,\textsuperscript{35} due to their extreme scale economies, the very strong network effect and their ability to collect data.\textsuperscript{36} Absent any form of regulation, dynamic efficiency is very likely to lead towards monopolisation or, at best, towards ‘monopolistic competition’ (competition for the market).\textsuperscript{37} The result could be a small number of big techs dominating the market in many jurisdictions, at least in the provision of certain services. This being the case, big techs could become gatekeepers.\textsuperscript{38} They might use their market power to impose financial services to be carried out exclusively using their networks, what would create a lock-in effect. By this way, big techs might reduce the resilience of the financial system.\textsuperscript{39}

As we have advanced, the question is whether we need a specific regulation for big techs. In fact, there is a European

\begin{itemize}
\item \textsuperscript{29} FSB (2020) The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions. Market developments and financial stability implications, 9 October, p. 3 [https://www.fsb.org/wp-content/uploads/P091020.pdf].
\item \textsuperscript{30} Nicholls, R. (2021) Regtech as an antitrust enforcement tool. Journal of Antitrust Enforcement, Volume 9, Issue 1, March, pp. 135 and ff.
\item \textsuperscript{31} Zetzsche, D., Arner, D., Buckley, R. (2020) The evolution and future of data-driven finance in the EU. CMLR, Nr. 57, p. 357.
\item \textsuperscript{32} Restoy, F. (2019) Regulating fintech: what is going on, and where are the challenges?. BIS, 16 October, pp. 2–3 [https://www.bis.org/speeches/sp191017a.htm (accessed 24 May 2021)].
\item \textsuperscript{33} Crisanto, J. C., Ehrentraud, J. and Fabian. M. (2021) Big techs in finance: regulatory approaches and policy options. FSI Briefs, N° 12, March, p. 3 [https://www.bis.org/fsi/fsibriefs12.pdf].
\item \textsuperscript{34} Marciano, A., Nicita, A., Ramello, G. B. (2020) Big data and big techs: understanding the value of information in platform capitalism. European Journal of Law and Economics, Nr. 50, p. 348.
\item \textsuperscript{35} Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15.12.2020, COM (2020) 842 final, para 2.
\item \textsuperscript{36} FSB (2019) BigTech in finance. Market developments and potential financial stability implications, 9 December, p. 1 [https://www.fsb.org/2019/12/bigtech-in-finance-market-developments-and-potential-financial-stability-implications/].
\item \textsuperscript{37} Marciano, A., Nicita, A., Ramello, G. B. (2020) Big data and big techs: understanding the value of information in platform capitalism. European Journal of Law and Economics, Nr. 50, p. 348.
\item \textsuperscript{38} Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15.12.2020, COM (2020) 842 final, para 2.
\item \textsuperscript{39} FSB (2019), BigTech in finance. Market developments and potential financial stability implications, 9 December, p. 2 [https://www.fsb.org/2019/12/bigtech-in-finance-market-developments-and-potential-financial-stability-implications/].
\end{itemize}
Commission proposal of a Directive on Digital Markets\textsuperscript{40} that, if passed, it would be applicable to financial services (investment, insurance and banking services, pension funds, etc.)\textsuperscript{41} provided by platform services providers designated as gatekeepers. The assumption is that gatekeepers have the ability and incentive to leverage their gatekeeper power to ancillary services (for instance, payment services), to the detriment of choice and contestability of these services.\textsuperscript{42} Data could be used for targeting advertising, undercutting prices or offering tailored services to clients.\textsuperscript{43} Under this premise, the regulation would oblige gatekeepers to refrain from unfair conducts, such as combining personal data at their disposal or limiting the services that business users might want to provide (Articles 5 and 6). In cases of systematic infringements, behavioural or structural remedies could be imposed (Article 16). The proposed regulation would apply irrespective of the place of establishment or residence of the gatekeepers (Article 1.2).

Regulation must prevent technology giants from unlawfully consolidating and exploiting their market power, but it must do so without hindering innovation.\textsuperscript{44} Sectoral regulation has many drawbacks, as utilities and network industries regulation shows. It is claimed that many of today’s proposals to regulate big techs seem to have forgotten lessons from the past.\textsuperscript{45} Economic activities should be deregulated as much as possible.\textsuperscript{46} However, it is also true that according to the experience, in many cases ex ante regulation is needed to protect the interests at stake. Competition law is often not sufficiently effective in markets where there is a persistent structural lack of competition. This might be the case. As described above, the proposed regulation could be an appropriate remedy to address the specific problems associated to big techs. It would not prevent the participation of large technologies in financial services, but would seek to ensure fair play in the provision of financial services.

\textbf{How to deal with crypto-assets, cryptocurrencies and digital stable coins?}

\textit{Crypto-assets} are digital representations of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology.\textsuperscript{47} Thus, they can be hold and traded in an anonymous and decentralised way. Crypto-assets can be used as a means of payment becoming cryptocurrencies. To avoid extreme volatility, stable cryptocurrencies refer their value to a legal tender (bitcoin, ethereum, litecoin).

The starting point is whether they should be considered as money. In this respect, it should be recalled that money has three main functions: (1) to be a reliable store of value; (2) a widely accepted means of exchange or payment; (3) and a unit of account to measure the value of goods and services. This being the case only stable cryptocurrencies could be considered as money. Other cryptocurrencies are highly volatile and are not generally accepted as a means of payment. It is true that the use of stable cryptocurrencies as a means of payment usually requires the intervention of intermediaries. However, this is already the case with electronic payment systems (cards).

Secondly, in a sense, cryptocurrencies have been “created to compete with central banks”.\textsuperscript{48} The question then arises as to whether money is a state monopoly. Strictly speaking it is, since central banks have monopoly rights to issue legal tender (official currency), also called sovereign money. This ensures uniformity, facilitates state supervision and gives central banks the ability to control the amount of money in the market, so that it can implement monetary policy. In the EU, the ECB has the exclusive right to authorise the issue of euro banknotes (Article 128.1 TFEU). Only the banknotes issued by the ECB and the national central banks are legal tender in the EU. However, money in the broad sense of the term is not a state monopoly.\textsuperscript{49} A very essential element of the financial system is commercial bank money, which is provided by the private sector (bank transfers, cheques, cards, credits). Moreover, nothing prevents other tokens outside the regulated financial system from qualifying as money. Indeed, money “is not only a social convention, it is a very dynamic one”\textsuperscript{50}.

\textsuperscript{40} COM (2020) 842 final.
\textsuperscript{41} COM (2020) 842 final, para 13.
\textsuperscript{42} COM (2020) 842 final, para 14.
\textsuperscript{43} Zetzsche, Arner and Buckley (2020), p. 345.
\textsuperscript{44} Marciano, Nicita, Ramello (2020), p. 355.
\textsuperscript{45} Wilson, C. S., Klovers, K. (2020) The growing nostalgia for past regulatory misadventures and the risk of repeating these mistakes with Big Tech. Journal of Antitrust Enforcement, Volume 8, Issue 1, March, pp. 10–29.
\textsuperscript{46} Laguna de Paz, J. C. (2012) Regulation and Competition Law. European Competition Law Review, Issue 2, p. 77.
\textsuperscript{47} Article 3.1(2) of the Proposal for a Regulation of the Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (COM/2020/593 final).
\textsuperscript{48} Raskin, M. and Yermack, D. (2018) Digital currencies, decentralised ledges and the future of central banking. In: Conti-Brown, P. and Lasra, R., Research Handbook on Central Banking, Elgar, p. 474.
\textsuperscript{49} Lasra, R. M. (2015) International Financial and Monetary Law, 2nd edition. Oxford: Oxford University Press, p. 13.
\textsuperscript{50} Cunliffe, J. (2021) Do we need ‘public money’?, 13 May [https://www.bis.org/review/r210517c.htm (accessed 17 May 2021)].
Thirdly, crypto-assets and cryptocurrencies are not currently regulated at EU level, nor in most countries. More precisely, they are subject to the general financial regulation.\textsuperscript{51} However, this does not seem sufficient. On the contrary, specific legislation may be necessary to avoid loopholes and to protect the interests at stake.

There is an increasing pressure for payment systems to be instantaneous and available round the clock. Cryptocurrencies provide easier, faster and cheaper means of payment. However, even stable cryptocurrencies remain highly speculative. Investors do not benefit from the guarantees offered by regulated financial services.\textsuperscript{52} They are not a liability of any entity. At the same time, payments are not secured, since they are made without the intervention of a trusted third party, in contrast to other digital currencies (Paypal). Adequate regulation and supervision is therefore necessary to protect users from the risks associated with these assets.

In addition, stronger regulation and supervision may be needed to prevent crypto-assets from being used for illegal purposes (money laundering, tax evasion, terrorism financing).\textsuperscript{53} In fact, a growing internet infrastructure dedicated to cybercrime is based on the use of cryptocurrencies.\textsuperscript{54}

Finally, specific regulation seems necessary to protect the financial stability.\textsuperscript{55} At present, the implications of cryptocurrencies for the financial system are limited. However, hedge funds investing in crypto-assets would need to be adequately supervised. Cryptocurrencies could lead to a strong market concentration, due to the network effects needed to be effective in this market. If they were widely adopted at international level, they could become systemically important in many jurisdictions (“global stablecoins”).\textsuperscript{56} The euro could be weakened if the bulk of deposits were in foreign digital assets.\textsuperscript{57} Moreover, cryptocurrencies could hamper the implementation of monetary policy.

With these reasons in mind, some states have recently passed some specific regulation for cryptoassets. Advertising of crypto-assets will generally be subject to licensing or disclosure obligations, such as warnings about risks and product features.\textsuperscript{58} The EU Commission has proposed a comprehensive “Regulation on Markets in Crypto-Assets”, which would provide legal certainty for issuers and providers of crypto-assets, as well as a pilot regime for market infrastructures to trade and settle transactions.\textsuperscript{59}

It is said that the world “appears to have been irreversibly changed by the arrival of algorithmic digital currencies”.\textsuperscript{60} Nobody knows whether this will really be the case. But most can agree that proper regulation and supervision seem necessary to reduce the risks of assets and currencies that are not backed by central banks.

Central bank digital currencies: In particular, the possible introduction of a digital euro

Most countries are considering the convenience of creating a Central Bank Digital Currency (CBDC). This is the case for the Eurosystem, the Federal Reserve, the Bank of England and other main actors. It is also very significant that some countries have already been involved in pilot projects (China, Switzerland, United Arab Emirates).\textsuperscript{61} The following comments refer in particular to the euro area, but could apply to a large extent to any other CBDC.

Last July, the ECB’s Governing Council agreed to launch a two-year “research phase”, at the end of which it will decide whether or not to issue a digital euro. The creation of a digital euro is an operation of extraordinary technical and organisational complexity, with serious financial and

\textsuperscript{51} FSB (2020) Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements, 13 October, p. 17 [https://www.fsb.org/wp-content/uploads/P131020-3.pdf (accessed 24 May 2021)].

\textsuperscript{52} ESMA Report on Trends, Risks and Vulnerabilities (2021), No. 1 [https://www.esma.europa.eu/sites/default/files/library/esma50-165-1524_trv_1_2021.pdf (accessed 24 May 2021)].

\textsuperscript{53} Coelho, R., Fishman, J. and García Ocampo, D. (2021) Supervising cryptoassets for anti-money laundering. FSI Insights on policy implementation, Nr. 31, April [file:///C:/Users/Usuario/Documents/JCLP%20MOIS%20DOCUMENTOS/BIBLIOGRAF%C3%BDA/BIBLIOGRAF%C3%BDA%20NUEVA/REGULACI%C3%B3N%20FINANCIERA/DIGITAL%20CURRENCIES/insights31.pdf (accessed 8 April 2021)].

\textsuperscript{54} The Economist (2021) New technology has enabled cybercrime on an industrial scale, 3 May [https://www.economist.com/international/2021/05/03/new-technology-has-enabled-cybercrime-on-an-industrial-scale (accessed 5 May 2021)].

\textsuperscript{55} Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final, p. 2 [https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF].

\textsuperscript{56} FSB (2020) Regulation, Supervision and Oversight of “Global

\textsuperscript{57} Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final [https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684].

\textsuperscript{58} Article 240 bis of the Royal Decree-Law 5/2021 of 12 March, which amends Royal Legislative Decree 4/2015, of 23 October, which approves the revised text of the Securities Market Law.

\textsuperscript{59} Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final (https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684).

\textsuperscript{60} Raskin (2018), p. 474.

\textsuperscript{61} https://www.bis.org/press/p210223.htm
monetary implications. However, it is very likely that its introduction will be agreed. There may be no alternative.

A CBDC might be necessary for sovereign money to keep fulfilling its function (“if we want to retain public money capable of general use and available to citizens, the state will need to issue public digital money that can meet the needs of modern day life”62). The ever increasing role of digital money issued by non-supervised institutions could replace central bank money. If most of the population would switch to private money, the central bank would lose its ability to control the money and to carry out monetary policy. This would be a completely new situation, which would alter the foundations on which the economy is based.

To avoid this situation, it is very likely that central banks in third countries will establish digital currencies, which could be made available to national citizens. From this point of view, an official digital currency could also contribute to safeguard the national economic autonomy.63

With all this in mind, it is very likely that the digital euro would not be limited to a wholesale market (for use by commercial banks), but would be opened up to retail use. In a digital global economy, an official digital currency could offer an efficient, safety, trustworthy and resilient payment system. A digital euro would ensure the availability of a means of payment in the event of a decline in the use of cash. Otherwise, in such scenario the payment system would need to rely exclusively on private payment solutions. Clearly, it could improve cross-border payments, the functioning of which is far from satisfactory.

However, the creation of a digital euro should consider carefully its many implications in order to avoid its potential drawbacks.

Firstly, it raises the question of whether it would require an amendment of the Treaty on the Functioning of the European Union (TFEU).64 In its wording, Article 128(1) TFEU confers on the ECB the exclusive right to authorise the issuance of euro banknotes, which are legal tender in the EU. However, legal provisions must be interpreted in accordance with the reality of the time in which they are to be applied, with particular regard to their purpose. The creation of a digital currency would not alter the mandate conferred on the ECB. “A digital euro would be just another way to supply euro, not a parallel currency”.65 It should be convertible at par with other forms of the euro (banknotes, central bank reserves and commercial bank deposits). In this sense, the right to issue “euro banknotes” shall be understood to encompass the right to determine the format or medium of such “euro banknotes”.66 Moreover, in a technological world a digital euro could be precisely the appropriate way to implement the monetary policy, entrusted to the ECB by Article 127(2) TFEU. Therefore, the digital euro would not require the amendment of the Treaties.

Secondly, we can assume that the digital euro could be used by a large part of the people, but not by all citizens. Digital innovation must not end up as a factor of social exclusion. This is why the digital euro should not replace banknotes and coins, but coexist with them at least for some time. Interoperability between CBDC and other forms of currency would need to be ensured.67

Thirdly, it would be necessary to minimise the incidence of the CBDC in the financial system to ensure that commercial banks and payment services providers keep playing a leading role in the economy. End users should not have direct access to the central bank. They should have access to the digital euro through intermediaries (entities which currently have access to central bank money).68 Commercial banks or payment service providers would be responsible for opening customers’ accounts at central banks and providing them with the corresponding retail services.69 To do otherwise would require a profound reorganisation of the institution. In that case, central banks should engage in providing end-user services, such as customer identification and support.70 However, in the long term, it cannot be ruled out that other players may also act as intermediaries between the central bank and end users (mobile operators, fintech, large technology companies).

Moreover, the transfer of funds to the ECB should be limited up to an individual threshold at any time.71 It should be borne in mind that holding digital euros would offer greater

---

62 Cunliffe, J. (2021) Do we need ‘public money’?, 13 May [https://www.bis.org/review/r210517c.htm (last visited: 17.5.2021)].
63 ECB (2020) Report on a digital euro, October, p. 14 [https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro--4d7268b458.en.pdf (last visited: 1.5.2021)].
64 Nabilou, H. (2020) Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies. Journal of Banking Regulation, vol. 21, pp. 299–314.
65 ECB Report on a digital euro (2020), October [https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro--4d7268b458.en.pdf (accessed 24 May 2021)], p. 7.
66 ECB, Report on a digital euro (2020), p. 25.
67 Kalifa Review of UK Fintech (2021), p. 29.
68 Bank of England (2020), Discussion Paper, Central Bank Digital Currency. Opportunities, challenges and design. March [https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1CSB18E63E71F68E4593].
69 Carsten, A. (2021) Central bank digital currencies: putting a big idea into practice, 31 March, 7–8 [https://www.bis.org/speeches/sp210331.pdf (accessed 24 May 2021)].
70 ECB Report on a digital euro (2020), p. 26.
71 ECB Report on a digital euro (2020), pp. 17 and 28.
security by foreign investors should be established. The digital euro would be a liability of the ECB, not of commercial banks. Financial intermediaries are regulated and supervised, so the risk is small, but they can fail and in that case the coverage of the deposit guarantee is limited. By contrast, the digital euro would be central bank money which by definition is risk-free. This is why it would be necessary to set limits on individual holdings of digital euros, or to discourage them above certain amounts. Otherwise, the digital euro could lead to a serious de-funding of the commercial banking sector. If significant deposit balances were moved from commercial banks into central bank, commercial banks would not be able to play their role as providers of credit, which is essential for the economy.

A digital euro should also be integrated into existing payment infrastructures. The digital euro should be interoperable with private payment systems. Innovations in retail payment systems should continue to come from the private sector.

Fourthly, a critical issue for a digital currency would be to ensure consumer privacy. Electronic payments raise privacy concerns that cash does not. Arguably, an official digital currency could guarantee privacy, unlike private payments, where services are usually offered in exchange for personal data that is then used for commercial purposes. However, full anonymity may not be guaranteed, as it could threaten anti-money laundering and anti-terrorist financing policy. It could also hamper monetary policy objectives, such as the need to control excessive capital flows from outside the euro area. However, anonymity could be guaranteed for limited amounts of money.

Fifthly, the digital euro implications for monetary policy should also be taken into account. The question arises as to whether the digital euro should be remunerated, in which case the ECB should be able to set the interest rate. In addition, limits and controls on the holding of the digital euro by foreign investors should be established. Otherwise, the digital euro could attract large capital inflows, which would affect its exchange rate, reducing the competitiveness of European industry.

In short, the digital euro should be designed in a way to ensure that it is an attractive means of payment, but avoiding its use as a form of investment and the associated risk of large shifts from bank deposits to digital euro. Finally, it will also be necessary to ensure international cooperation, which is essential to guarantee the stability of the financial system, the convertibility and interoperability of digital currencies and the effectiveness of means of payment.

Conclusions

First, in a global digital economy, where citizens are increasingly dependent on services provided by big techs, consent-based protection of personal data might not be an effective way to protect the fundamental rights at stake. In this respect, it might be appropriate for legislation to provide more safeguards for the processing and transfer of personal data.

Second, financial business is expected to rely increasingly on big data and AI. The question is to what extent commercial decisions can be based on gender, age, tastes or consumption patterns. Commercial banks are private companies that seek to make a profit. In doing so, they also contribute to preserving financial stability and to the public good. However, some limits to the use of personal data may derive from the fundamental rights at stake. Where appropriate, it would be a task for legislators to set limits on the commercial freedom of financial actors, who would otherwise be able to make their decisions as they see fit.

Third, central banks and supervisory authorities are increasingly using new technologies to exercise their regulatory and supervisory competences. However, the mere use of new technological tools -including machine learning and AI- do not seem to alter the legal foundations of financial supervision.

Fourth, it might be appropriate to pass a specific regulation for big techs holding a gatekeepers’ position to ensure financial stability, a level playing field between operators and consumer protection. In fact, the proposed Digital Markets Directive, if adopted, would apply to financial services provided by big techs.

Fifth, a specific regulation for crypto-currencies seems necessary to protect consumers and eventually the financial stability. This is why some countries have passed some

---

72 Raskin (2018), p. 485.
73 Bank of England (2020) Discussion Paper, Central Bank Digital Currency. Opportunities, challenges and design, March, p. 5 [https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD186464A7CC0772AF1C5B18E63E71F68E4593].
74 ECB Report on a digital euro (2020), pp. 20–21.
75 Maechler, A. M. and Moser, T. (2021), COVID-19, financial markets and digital transformation. Money Market Event, 15 April, p. 7 [https://www.bis.org/review/r210415d.pdf (last visited: 15.4.2021)].
76 Kalifa Review of UK Fintech (2021), p. 29.
77 Panetta, F. (2021) A digital euro to meet the expectations of Europeans. Introductory remarks, 15 April, p. 2 [https://www.bis.org/review/r210414h.pdf].
78 ECB Report on a digital euro (2020), p. 27.
regulation on this subject and there is a proposal to regulate it at EU level.

Sixth, the creation of an official digital currency might be necessary for sovereign money to continue to fulfil its role in a digital world. However, it should carefully consider its multiple implications in order to avoid its potential drawbacks. In particular, it should seek to minimise its impact on the financial system to ensure that commercial banks and payment service providers continue to play a strong role in the economy.

Declarations

Conflict of interest The author declares that there is no conflict of interest.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

José Carlos Laguna de Paz is a professor of Administrative Law at the University of Valladolid (Spain). He has published and edited numerous books and articles on regulation, competition law, public procurement and services of general economic interest (financial sector, telecom, energy and media). He has been a visiting professor and taught in many universities. He has consulted for European and Latin American supervisory bodies and private corporations. He is a member of Scientific Associations, University Institutes and Professional Associations.