FinTech, regulation, and cybercrime: opportunities arising from new technologies

Monica Violeta ACHIM[1], Galena PISONI[2], Codruta MARE[3*], Maria MOLONEY[4], Szabolcs KORBA[5], Balint MOLNAR[6], Barbara BĘDOWSKA-SÓJKA[7], Ioana COITA[8]

[1]Dep. of Finance, Faculty of Economics and Business Administration, Babes-Bolyai University, Cluj-Napoca, Romania

[2]Université Cote d'Azur, Polytech Nice Sophia, Campus ShopiaTech

[3]Dep. of Statistics, Forecasts, Mathematics, Faculty of Economics and Business Administration, and the Interdisciplinary Centre for Data Science, Babes-Bolyai University, Cluj-Napoca, Romania

[4]University College Dublin, Belfield, Dublin 4, Ireland

[5]Bifröst University, Iceland

[6]Information Systems Department, Faculty of Informatics, Eötvös Loránd University of Budapest, ELTE, Budapest, Hungary

[7]Poznań University of Economics and Business in Poland, Department of Econometrics, Poznań, Poland

[8]University of Oradea - Faculty of Economic Sciences, Oradea Romania

*corresponding author: codruta.mare@econ.ubbcluj.ro, codruta.mare@ubbcluj.ro

Acknowledgement: This paper is part of the project COST CA19130 FinAI - Fintech and Artificial Intelligence in Finance - Towards a Transparent Financial Industry and was supported by a VMG grant from this COST Action.

This work was supported by a grant of the Romanian Ministry of Education and Research, CNCS - UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174, within PNCDI III.

Codruta Mare acknowledges that this work was supported by the project "**A better understanding of socio-economic systems using quantitative methods from Physics**" funded by the European Union – NextgenerationEU and the Romanian Government, under National Recovery and Resilience Plan for Romania, contract no 760034/23.05.2023, cod PNRR-C9-I8-CF255/29.11.2022, through the Romanian Ministry of Research, Innovation and Digitalization, within Component 9, Investment I8"

Abstract

The main goal of this work is to address the main issues that derive from the adoption of Financial Technologies (FinTech). We conduct a bibliometric and systematic literature review to assess the theoretical background on the subject matter based on the specialized literature, in a way that elucidates the reasons for the topic's significance, ultimately revealing the research gap that this study intends to address. We discuss important topics related to FinTech, such as the advantages and risks, the huge need for regulation, the need for financial inclusion, the increased risks given to the financial transactions and how to face these cybercrimes within potential solutions. We also explore how financial companies can use new technologies to create new services and products using the large amount of data they have. We present the implications of our work for policy makers from different levels - microeconomic, macroeconomic, and European level.

1.Introduction

In recent years, the financial industry has experienced significant changes. This has happened because there is more data available all over the world. Big Data has led to advancements in Artificial Intelligence (AI) and Machine Learning (ML) technologies and use, automation, and new ways to predict human behaviour. But this is not only limited to the financial industry. AI is being used more and more and is doing well in many areas. Artificial Intelligence (AI) is changing how entire industries and businesses work. New smart services are ideated continuously. For instance profiling and social scoring study how customers behave and come up with new and creative products and designs (Chamorro-Premuzic, Polli & Dattner, 2019; Kiron & Schrage, 2019). Nowadays, market segmentations, or for instance sentiment analysis, or operations of rapidly trading stocks are usually done by computers. Chatbots are taking over the jobs of customer service operations, AI models are figuring out credit scores, and most of us use online apps to pay when purchasing. The use of AI in Finance has increased a lot, especially because of the Covid-19 pandemic when people had to use technology to stay home and prevent spreading the virus.

As a result, there has been a huge increase in the number of people using apps like Google or Apple Pay. There has been a big increase in FinTech start-ups that are trying to use technology to do online transactions that people usually do. In the business world, companies have started using AI and ML tools instead of relying on cash flow and managing employees

manually. According to IBM (2022), more than 35% of the companies worldwide were using AI in their daily activities in 2022, while almost 80% stated they intend to introduce AI in their activities. This transition from humans making decisions and managing things to relying on technology has led to some problems with keeping information safe. This leads us to another important way that AI and Machine Learning are used in finance. Artificial Intelligence (AI) is used to protect against computer security issues, identify and prevent fake activities, and detect and stop financial crimes. Thus, cybercrime comes into force and protection against it becomes crucial.

The following section encompasses a bibliometric and systematic literature review to assess the theoretical background on the subject matter based on the specialized literature, in a way that elucidates the reasons for the topic's significance, ultimately revealing the research gap that this study intends to address. We discuss important topics related to FinTech, such as the advantages and risks, the huge need for regulation, the need for financial inclusion, the increased risks given to the financial transactions and how to face these cybercrimes within potential solutions. All these issues are the object of section 3 where a systematic literature review is conducted for these topics. Section 4 provided discussion, policy implications, and the path forward. The paper ends with the conclusions of the work.

2. Bibliometric analysis of the articles on the topic of FinTech

Methodology and data

As the main source of our research, we used the collection of studies published in the Web of Science Core Collection in the period between 1975 and October 2023 with FinTech as the theme. First, the word "FinTech" was used as a search key. Works in the sample were classified using descriptive statistics tools based on fields of research, the countries where they were developed and the year of publication, using data from the WOS analysis. Subsequently, we employed the VOSViewer software tool to create and explore connection maps.

To create a connection map, the main steps followed were: choosing the data source, namely the bibliographic data text file; choosing the fields where the search is made, respectively in the keyword field in the case of our research; choosing the number of occurrences of FinTech related terms - five appearances. The program calculated and displayed both the strength of the links between the terms and the number of occurrences of each keyword and finally the map was generated.

Results and discussions

The evolution of the number of scientific articles with the topic of FinTech is presented in Figure 1. A sharp increase in the number of publications over the time is emphasized, with only 2 papers published in 2015, but a huge jump to 334 articles in 2023. We may note the concern on this topic registered the highest growth rate in 2022, when the number of publications raised from 189 (2021) to 311 (2022), thus an increase of about 1.6 times. The explanation should be found in the COVID-19 pandemic period that asked for a huge level of digitalization in economy.

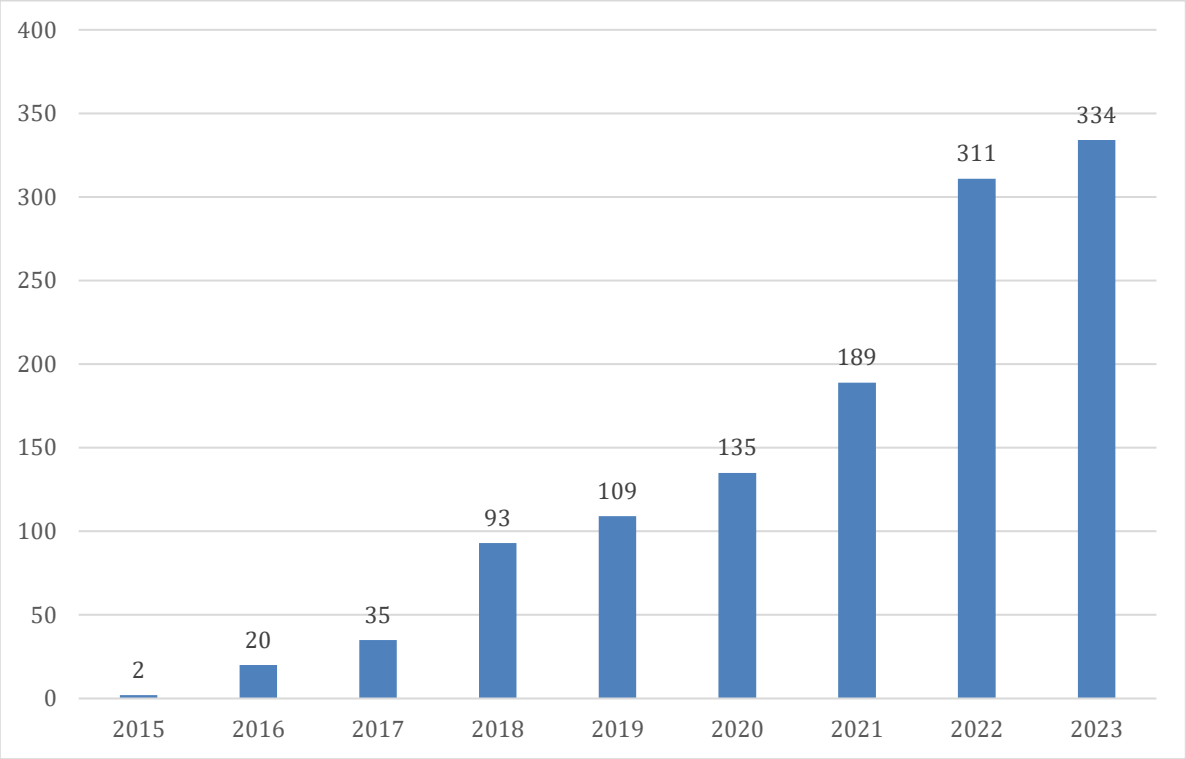

Figure 1. Distribution of FinTech scientific articles by year of publication

Source: authors' construction

Figure 2 describes the top 15 research fields based on the number of scientific articles according to the WOS category classification. As expected, the field of Business & Finance is on the 1st place, with the highest number of 220 articles published on the topic of FinTech. It is naturally followed by "Economics" (92) and on the third place by "Business" (79). It is worthy to note the fourth place occupied by "Law", which demonstrates the interest of scientists in the investigation of regulation framework in this field (58).

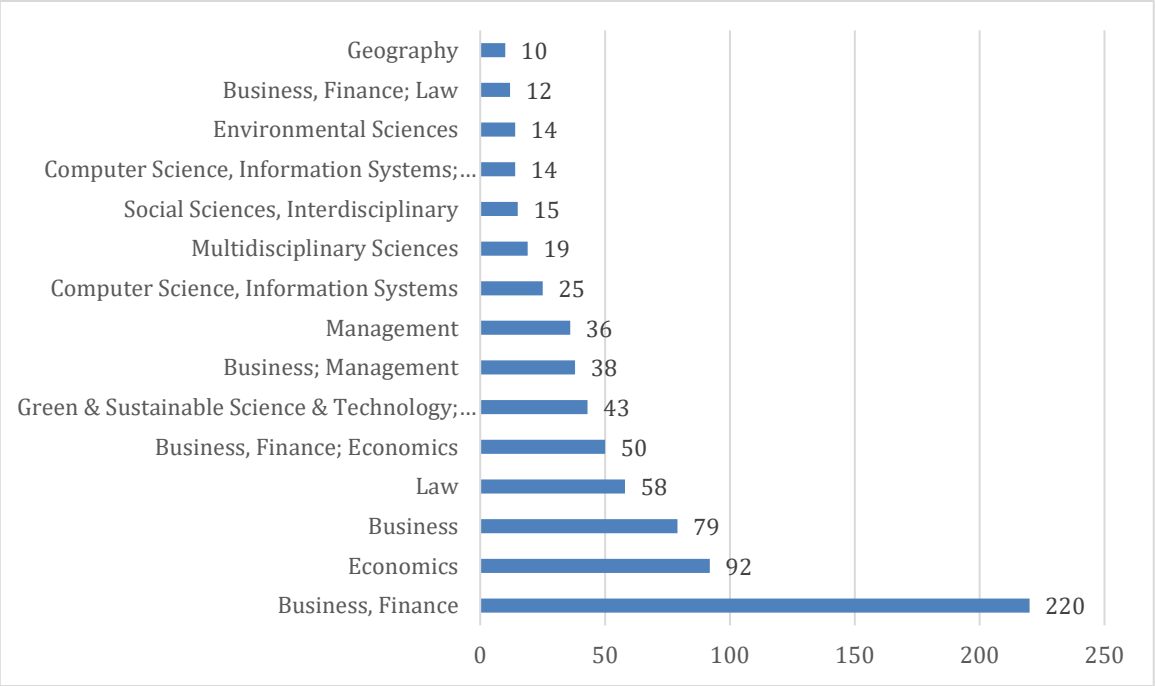

Figure 2. Distribution of FinTech scientific articles by research field

Source: authors' construction

In Figure 3 the distribution of scientific articles with the topic of FinTech by Journals is reflected. It is interesting to see that the journal Sustainability has published the highest number of papers on the topic of FinTech - 44, up to the moment of the analysis. It is followed on the second place by Finance Research Letters (with 30) and by Financial Innovation (with 24) on the third place.

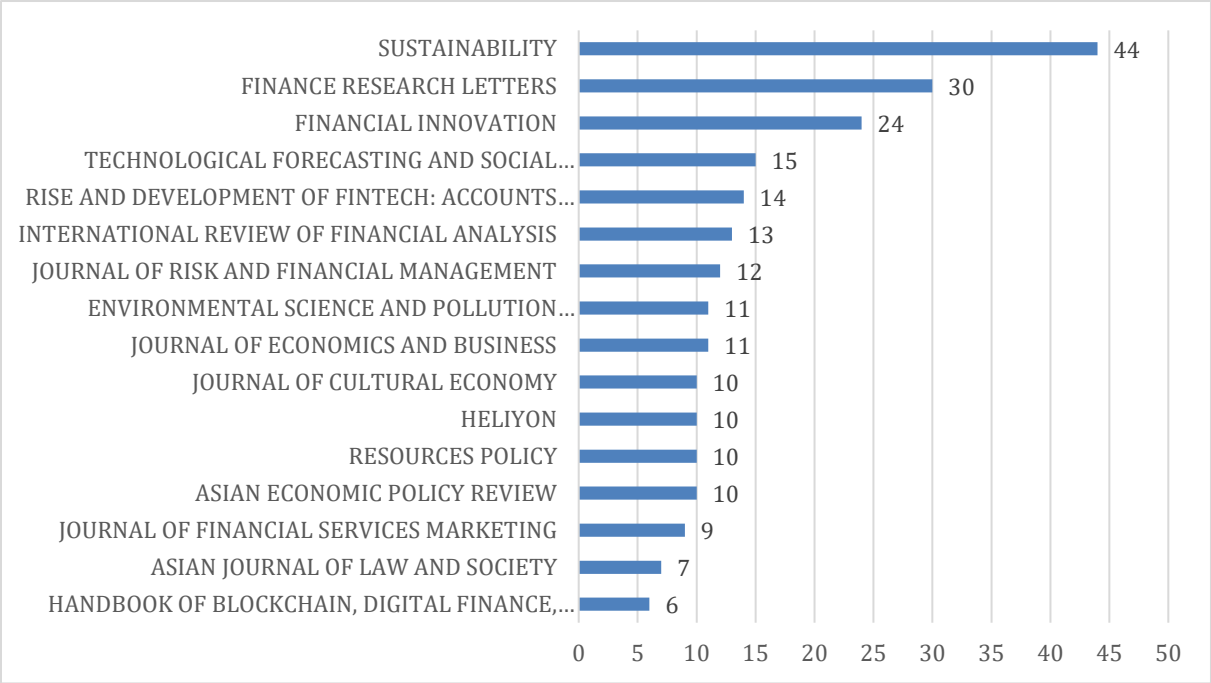

Figure 3. Distribution of FinTech scientific articles by Journals

Source: authors' construction

Also in relation with the journals, Figure 4 helps to analyse the presence of bibliographic coupling by Journals. These clusters are built depending on the frequency of use, connexions and strength of connexions. Sustainability, even if it is the journal that has published the highest number of papers on the FinTech topic ever, it is in the cluster with few journals such Journal of Cleaner Production, Environmental Science and Pollution Research and Resource Policy with which there were identified important co-occurrences between keywords. Then, another important cluster has in a central place the journal Finance Research letter with important co-occurrence with Electronic Commerce Research, European Journal of Finance or International Review of Finance Research in International Business. A third cluster is centred in the Journal of Economics and Business, but the differences from other journals are not important. Any other journal such as Journal of Cultural Economy, Rise and Development of FinTech, Asian Economic Policy Review or FinTech, Artificial Intelligence and the law- Regulation and Crime Prevention are of a high importance from the point of view of co-occurrence of the keywords.

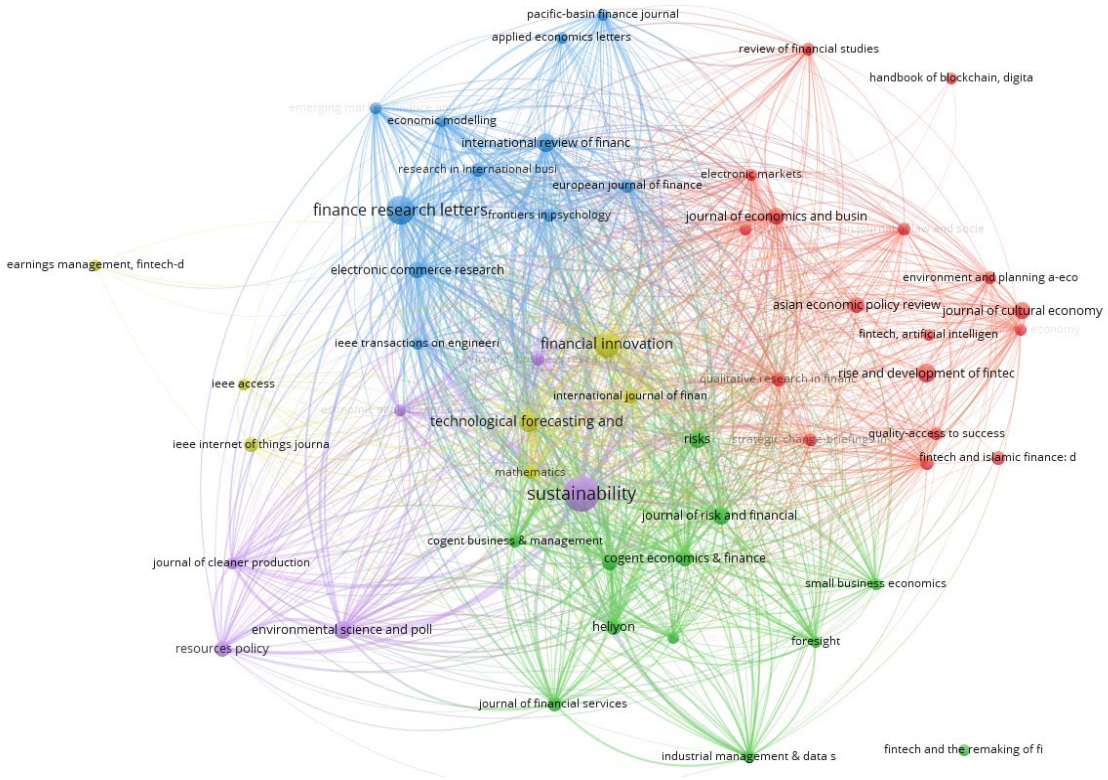

Figure 4. Bibliometric analysis using the keywords “FinTech”. Bibliographic coupling by Journals

Source: authors’ construction

Figure 5 reflects the results obtained by using VOSviewer in order to identify the most common keywords used in relation to FinTech. We select the number of occurrences of a related keyword to be at least 20. Thus, we identify five main clusters of co-occurrences. The green cluster puts FinTech in relation to the terms “financial regulation”, “financial stability”, “innovation” and “financial inclusion” as being the most related terms with common co-occurrence. Then, we may read the red cluster that belongs to the sectors of “banking and finance” where terms as “artificial intelligence”, “regulation”, “big data”, “risk”, “credit”, “competition” and “market” dominate this cluster. A special cluster with common patterns and occurrence is seen in yellow. It reunites terms such as “cryptocurrency”, “bitcoin”, “blockchain” or “financial services”.

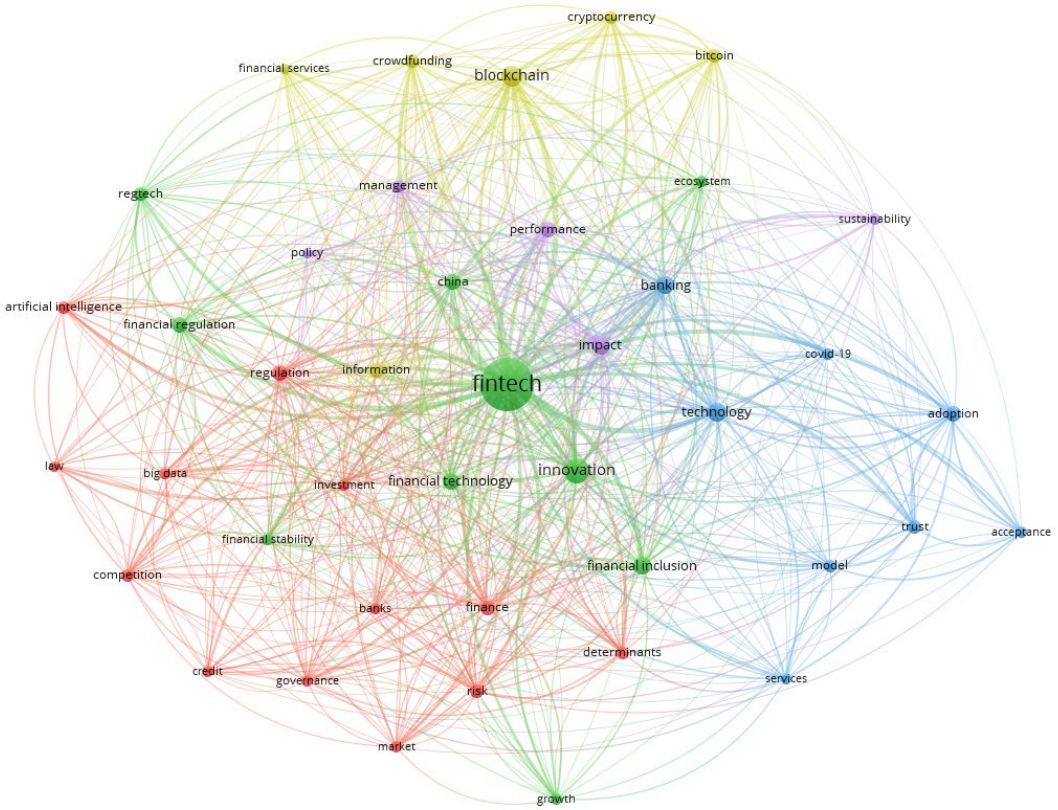

Figure 5. Bibliometric analysis using the keyword “FinTech”. Co-occurrence of keywords.

Source: authors’ construction

Figure 6 presents a bibliometric analysis using the keyword “FinTech” that connects publications in clusters using bibliographic coupling by Countries. We may observe that three main countries dominate the bibliographic coupling such as China, The United Kingdom and then The United States. Then important production of cited research is realized by the high-income countries such as Australia, Netherland, Italy and Germany.

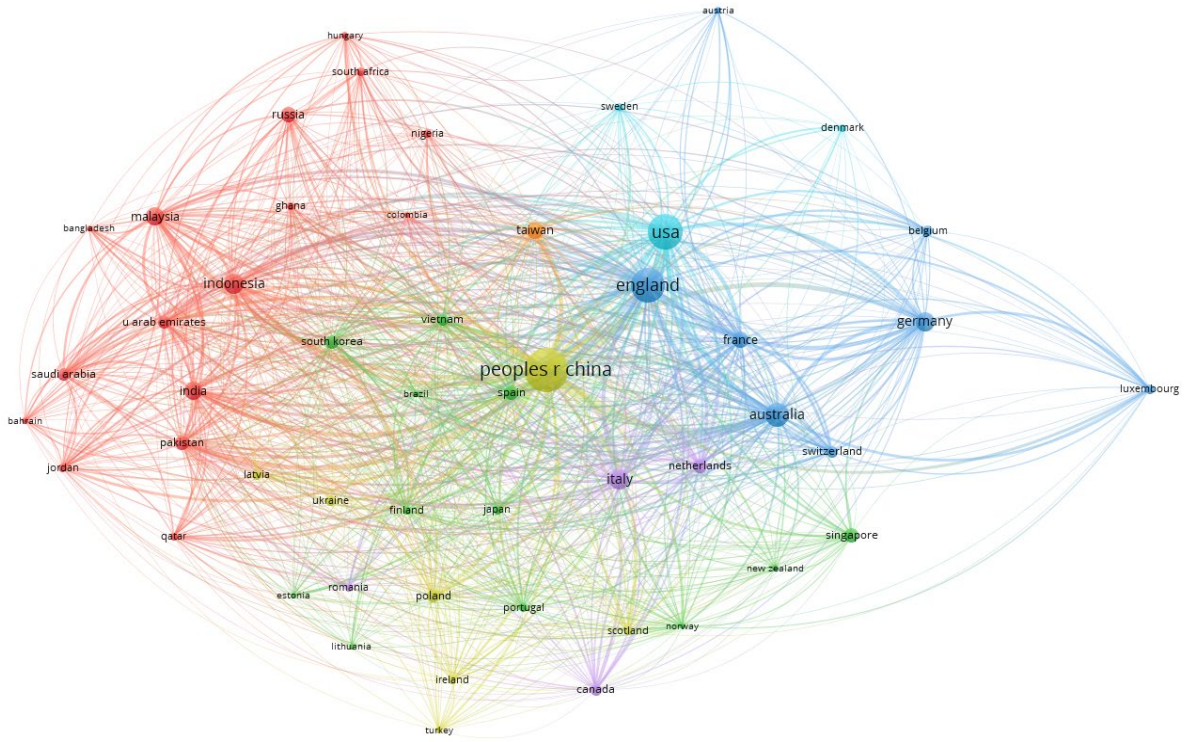

Figure 6. Bibliometric analysis using the keywords "FinTech". Bibliographic coupling by Countries

Source: authors' construction

The bibliometric analysis conducted on the FinTech literature highlights important topics in relation with it, such as the huge need for regulation, the need for financial inclusions, the increased risks given to the financial transactions and the way to counteract them, among others.

3. Systematic literature review

3.1 FinTech opportunities and risks

Higher levels of FinTech usage have clear advantages that can be represented by greater accessibility, time optimization, variety of services, cost reduction, reducing classical frauds, just to name some.

In respect to reducing classical frauds such as tax evasion, corruption, shadow economy, etc., the FinTech sector and its applications may contribute to the reduction in cash turnover and thus make monitoring of financial transactions much easier, through decreasing shadow economy (Remeikien et al. 2021; Elgin and Oyvat, 2013), and tax evasion (Immordino and

Russo, 2018, Okunogbe and Pouliquen, 2018, Coita et al., 2023a, 2023b). Moreover, technology may discourage corruption-engaging activities by reducing the interactions between the taxpayer on the one hand, and the representative of the tax authorities on the other hand (Slemrod, 1990; Bird & Zolt, 2008; Goel et al. 2012; Achim et al. 2021). These studies show internet diffusion to be associated with less corruption. In financial markets, the need of higher investments in regulatory technologies (RegFin) is highly required in order to reduce financial markets frauds (Williams, 2013; RegTech). In banks, credit card frauds are detected using various anti-money laundering techniques, especially based on artificial intelligence, while for detecting frauds in financial statements the best performing methods are probabilistic neural networks and genetic algorithms (Sadgali et al., 2019). Similar technologies consisting in computerized data mining programs, machine learning, and several tools for risk profiling are used to trace illicit funds for money laundering or terrorist acts (Levi & Wall, 2004; Amoore & de Goede, 2005; de Goede, 2008; Williams, 2013).

While above we have pointed out the positive usage and effects of FinTech upon the society, there is also the *dark side* of FinTech upon economy. While the society becomes more and more digital, organizations around the world are increasingly vulnerable to cyber threats. In 2020 alone, cybercrimes created a trillion-dollar global business loss. The problem will only escalate: 57% of organizations report unfilled cybersecurity positions, and the global cybersecurity workforce is short some 3.5 million workers in 2021, according to Cybersecurity Ventures. Concern over the dearth of tech talent, in general, is coming to a head as organizations are more and more relying on the digital environment and Digital Finance. With cybercrime on the rise, the shortfall in cybersecurity is particularly urgent. Thus, digitalization has also a dark side by facilitating new channels for fraudsters to gain illegal benefits when operating in digital space under the forms of cybercrime, bank fraud, FinTech frauds, e-commerce frauds etc. Under this context, all the economic and financial activities have suffered a high movement from traditional channels to online channels.

In this context, the term “digital shadow economy” has recently emerged in the literature as an expression of the frauds conducted in the digital space. In the broad sense, the “digital shadow economy” term is frequently aligned with the terms of “digital underground economy” and “digital black market”, respectively meaning profit-driven Internet-based unregistered activities (Herley and Florencio 2010) and illegal revenues generated as a result of online trade and service provision (Zorz,2015). Digital shadow economy refers to cybercrime, e-piracy, e-fraud, bank frauds, e-commerce (Remeikiene et al. 2021). Considering the illegal nature of

digital shadow economy, it is closely related to the concept of cybercrime, which is interpreted as Internet-based crime, conducted remotely to illegally take wealth or resources from others (Smith, 2015; Reimeikiene, 2018). According to the Global Economic Crime and Fraud Survey provided by PwC (2020) a share of 34% of frauds is conducted under the form of cybercrime, being on the second place after the consumer frauds (with 35%). Romania is among the top four most vulnerable countries in EU at cybercrime attacks after Slovenia, the Czech Republic and Bulgaria (Global Cybersecurity Index, 2020). Regarding bank frauds, statistics show an increase of fraud incidents over time. Thus, fraud losses per 100 U.S. dollars of total card sales worldwide have increased by 57 % in 2021 compared to 2010 (from 4.1 in 2010 to an estimate value of 7.1 in 2021) (Nilson, 2020). ATM malware and logical attacks against ATMs were up 269% in the first six months of 2020 compared to the first six months of 2019 (from 35 to 129) and all the reported attacks were Black Box attacks. The financial losses went up from less than €1,000, to just over €1 million (EAST, 2021). In the area of FinTech frauds it's worth mentioning Revolut, one of the world's most popular FinTech start-ups, that has been accused of violating basic banking rules and failing to block thousands of potentially suspicious transactions on the platform, favouring money laundering transactions (Finews, September 2020). Also in the FinTech area, it is worth mentioning that cryptocurrency transactions are suspected of hiding cash from the economy, as long as they are made under anonymity conditions (Crawley, 2021). According to the Federal Trade Commission (2021) USA consumers have reported losing more than $80 million to cryptocurrency investment scams, an increase of more than ten-fold year-over-year. People between the ages of 20 and 39 were hit particularly hard, representing about 44% of the reported losses. Fast-Growing E-Commerce attracts many types of frauds such as Chargebacks, Friendly fraud, Gaming and wireless fraud Account Takeover (ATO) (Columbus, 2020). There is clear evidence that cryptocurrencies and cybercrime are linked, so laws pertaining to cryptocurrencies and cybercrime must be coordinated. Insofar as international entities possess the legal structure and resources necessary to act swiftly in order to stop, deter, or combat criminal slippage, their rights and obligations must be re-examined (Scheau et al. 2020).

Regarding e-piracy, nearly a quarter of the global Internet bandwidth is used for online piracy. Every year 230,000 to 560,000 jobs are lost in the United States due to online video piracy (Statista, 2017). Despite efforts to curtail piracy, the latest piracy reports indicate that global film piracy increased by 33% during the COVID-19 lockdown (Go-gulf, 2021).

Among the dark faces of digital economy, we may mention the loss of privacy data, i.e. „the destruction of privacy in an unprecedented and irrevocable manner" (Trapscott, 2015). In this view the recent term of "surveillance capitalism" rises up in literature (Zuboff, 2019) and requires higher protection through a stronger *General Data Protection Regulation (GDPR)* framework. According to a January 2021 survey of worldwide adults, 66% of total respondents agreed on feeling that tech companies hold too much control over their personal data (Johnson, May 11, 2021). With more countries introducing modern privacy laws in the same vein as the General Data Protection Regulation (GDPR), the world has reached a threshold where the European baseline for handling personal information is now the de facto global standard. According to Gartner, Inc. by 2023, 65% of the world's population will have its personal data covered under modern privacy regulations, up from just 10% in 2020 (Gartner,2020). Additionally, the new AI Act is under consultations in the European Parliament, to ensure the proper treatment of personal data when AI tools are applied.

There is a common feature in modern cyberattacks: in most cases, basic computer hygiene such as keeping software updated, using strong passwords, encrypting sensitive data, and keeping copies in the cloud are sufficient to protect computers from such incidents. For example, one often-overlooked aspect of the 2017 WannaCry attack is that, even though more than 400,000 computers in over 150 countries were hit, millions were not affected because they had updated their software. For this reason, WannaCry was defined as a "tribute to negligence". As mentioned in the 2017 High Level Group of Scientific Advisors on Cybersecurity to the European Commission, many Europeans still fail to take basic cybersecurity measures: many say they care a lot about their personal data, but then give them away for free on social networks. Data are striking: 90% of the data breaches reported by the 2017 Verizon Data Breach Investigation were the result of phishing. And for those who are successfully phished it is not over, because they can expect it to happen again at least once during the same year. Cybersecurity should therefore become a collective responsibility and cyber awareness and computer hygiene should become an integral part of digital literacy programs. Without awareness-raising campaigns and smart policies, cybersecurity will always be dogged by collective action.

The European Union has launched the Digital Europe Programme for 2021-2027 and it proposes €9.2 billion to build the strategic digital capacities of the EU and for facilitating the wide deployment of digital technologies in supercomputing, artificial intelligence,

cybersecurity, advanced digital skills, and ensuring a wide use of digital technologies across the economy and society (European Commission, May 27th 2020).

3.2 European regulations for new tech and finance

GDPR mandates that the companies are responsible for how they use and protect personal data. Data controllers must show that they handle personal data responsibly and make fair decisions. They must also be transparent about how they collect data and only use it for specific purposes. They should store data for a limited time and make sure it's accurate. Lastly, they must keep personal data confidential. This is all part of the GDPR regulations set by the European Union in 2018. Companies in the European Union or those that handle personal data of European citizens, must follow the General Data Protection Regulation (GDPR) to make sure they are handling personal data in a legal and transparent manner. The main set of requirements for the companies are: companies must show that they have a lawful basis for processing personal data, must provide transparency in the processing activities, must ensure that they only process personal data that is necessary for the specific purpose, they must use accurate data, organizations need to use proper technology and methods to keep personal information safe, and must comply with data subject rights.

The European Union's Artificial Intelligence Act (AIA, 2023) requires that AI technology be regulated based on the level of risk it poses. This means that those who create and use AI are responsible for the choices made by the AI they use. The rule controls AI programs depending on how risky they are. This text is saying that there are rules for companies that make AI programs that are considered to be risky. These companies have to meet certain requirements before they can sell their AI program. The application will be continuously reviewed as long as it is available for sale. The levels of outlined risks are: no risk, limited risk, high-risk, and unacceptable risk. The AI Act imposes that companies that are creating AI should first evaluate the possible risks. Then, they should test the AI extensively to make sure it is safe, accurate, and secure from cyber threats. They also need to carefully manage their human resources, making sure that employees are suitable for their roles, do not accept bribes, and have strong ethical values. Lastly, the company should provide a detailed document explaining how the AI operates.

DORA is a law by the EU that deals with risks in technology, security, and infrastructure in the finance field. This law sets special rules for keeping the network and information systems of financial companies and organizations safe. It also applies to third-party companies that

provide services like cloud computing or data analysis. Financial companies must respond to and recover from all types of disruptions and threats related to technology. This helps prevent damage to security and infrastructure.

Market in Crypto-Assets (MiCA) and Decentralized Finance (Defi) are new laws by the European Union. These laws are designed to regulate crypto assets and other types of digital assets (like NFTs) that are not currently regulated by existing financial laws. This is the first time customers are protected from the dangers of these new digital assets. The regulation includes different aspects like being open and clear, giving permission, and making sure everyone follows the rules when buying and selling. With this law Europe has been a pioneer in protecting rights in the field of cryptocurrencies.

PSD2 law focuses on payments. It creates strict rules regarding keeping electronic payments safe and protecting people's financial information. The goal of putting it into action is to encourage competition and innovation in electronic payments, to make payments safer and more secure, and to improve customer protection, by making sure that both communication and people's information are safe.

MiFID II law regulates financial products and how financial companies operate. People who sell finance products have to show that they acted in the client's best interest, keep records of their work for the client, and be clear about any gifts or benefits they receive from others that could affect how they do business with the client. It sets guidelines that companies must follow to ensure fair business practices and protect the customer's rights. The goal is to prevent fraud, deception, or any other practices that may harm the customer's best interests. Article 13 in the EU AI Act (AI Act 2023) is about being open and giving clear information to users.

The main responsibilities that come from current rules are related to the fact that digital finance companies need to prove that they work in the customer's best interests and keep a record of how they do so. In simple words, they need to show that they have been open, honest, and professional in dealing with customers. They also need to provide complete and clear information about their finances, including any involvement with other companies and their responsibilities towards them. If there are other companies involved, they must explain who they are and what they need to do. Furthermore, it is important to clearly explain how the fee for the financial product works.

For companies, it is important to establish and update policies that protect the customer's best interests. They should also provide the customer with clear information about fees, benefits, obligations, and commissions.

3.3 Financial inclusion and social responsibility of finance

Financial inclusion is a goal that the European Union is trying to achieve. Although we have come a long way in the development of technical tools for using available data on the internet, we still have categories of people that do not have access to either financial services or capital. We are not there yet for a variety of reasons, including discrimination, bias in data and models, demographic conditions, financial literacy, and others. Financial inclusion goes hand in hand with the big tech players, who have access to large volumes of data and are building smart tools for profiling various sectors, not just the financial one. Moreover, we have large players in the financial domain who benefit from the services of technology companies in order to develop online risk assessment tools in countries like the USA, UK, or China. Firstly, there are the regulatory aspects that the banking sector needs to comply with, like Basel III or IV, regarding risk and credit data. This norm has the purpose of protecting consumers as end users of financial services from cyber-attacks or fraud. In this context, FinTech companies started to offer alternative financial services in a way that was more democratic, cheaper, and quicker. This increased the rate of financial inclusion for under-represented groups but did not solve the problem of getting access to the capital needed in a more inclusive way. The most recent research on alternative data sources shows that they are increasingly being used by lenders to evaluate credit applications in order to lower costs and get more financing (Jagtiani & Lemieux, 2019; Misheva, Osterrieder et al., 2021; Rosenblatt, 2020). The authors analysed traditional credit ratings, bank account transactions, insurance claims, credit card transactions, the consumer’s occupation, education, use of mobile phones, internet footprints, online shopping habits, investment choices, and others. Financial inclusion is a driver of growth, and the FinTech sector is promoting it (World Bank, 2022).

Thus, the way statistical risk analysis tools are currently used in financial organizations and institutions reveals substantial oversights that limit our understanding of the consequences of potential bias and model frailty. Considering that AI (Artificial Intelligence), among others, is expected to adopt various tasks in finance and across a variety of contexts and financial jobs in the future, millions of employees will be confronted with this new form of technology. To ensure that those making decisions based on AI and those that are affected by these very

decisions can perform at a high level and feel their financial needs are addressed, it is therefore imperative to investigate the consequences of AI tools in risk management and financial resource provision. A sustainable, competitive, and resilient economy needs to rely on a sound, secure, reliable, and innovative financial industry as their backbone. To develop a common European market to its full potential, it is paramount to ensure equitable access to finance, access to new financial instruments, sound and reliable data for financial decision-making to facilitate the function of markets, and in particular, adequate financial support to allow startups, SMEs, and large corporations to prosper. An innovative and competitive European financial sector is therefore vital for the transformation and modernization of the common European economy across sectors.

In this sense, current research is looking at the following problems: Are these models biased in the predictions they make? Is the data used to feed these models biased? Would solving these problems address the real cause of discrimination? Moreover, improving existing traditional tools for measuring risk would still leave a large population of disadvantaged people without access to capital. There are numerous reasons for this, including people who lack collateral or do not have sufficient transaction histories; tech start-ups that do not stick to predictions because they are high-risk, high-gain, and so on. Presently, in the lending sector, companies are evaluated based on their financials, and the riskier the company, the higher the cost of debt. Tackling the gender bias challenges posed by this type of alternative risk scoring model is not an easy challenge. Firstly, there is the protection of personal data that is used to feed and build these models. Models of this type should be ethical, respect people's right to privacy, be transparent, reliable, and trustworthy, and ensure that sustainable companies get financed according to the EU's Green Deal. European legislation on data protection is a step forward in this field together with other European initiatives involving the use of personal data by algorithms, like the European approach to AI that encourages the development of human-centric and trustworthy models. They should also treat bias in a fair manner so as to ensure access to capital in a more inclusive manner. At the European level, there is also the Gender Equality Strategy, which targets the achievement of gender balance in fields where women are under-represented. FinTech services make access to finance easier, faster, helping drive financial inclusion, but their impact on gender gaps varies across countries (Khera et al., 2022). Another study found that FinTech use has a greater impact on closing the gender gap than traditional financial services (Yoke Wang & Heng, 2022). Using gender modeling, Kelley et al. (2022) find out that it reduces discrimination. AI models used for this purpose should include

human judgment in the process of achieving results in order to effectively treat discrimination (Silberg & Manyika, 2019).

European Commission supports the use of artificial intelligence in the provision of financial services. The purpose is to ensure financial stability, protecting savers' and lenders' rights by combating financial fraud and ensure that businesses and consumers have greater access to capital needed. European Commission (EC) and other public institutions including European Securities and Markets Authority, European Central Bank, Financial Stability Board together with national financial institutions are working to adapt the legal framework to innovative FinTech financial services. Moreover, EC is working on introducing Big Data to the official statistics system.

3.4 FinTech, cybercrime, and potential solutions

As we mentioned before, there are various advantages of Artificial Intelligence, including faster access to information, improved customer experience, increased productivity, lower operational costs, improved decision-making, improved information security, higher mobility, automation of business processes, agility, and disaster recovery.

Digital solutions

To tackle these challenges, financial institutions and regulatory authorities have implemented various digital solutions that use advanced technologies such as Artificial Intelligence (AI), Machine Learning (ML), and blockchain to detect and prevent financial crimes. Regarding anti-fraud technologies, the detection of credit card fraud uses various money laundering techniques, especially those of Artificial Intelligence, while for detecting frauds in financial statements, the best performing methods are Probabilistic Neural Network and Genetic Algorithms (Sadgali et al., 2019). Similar technologies consist in computerized data mining programs, ML and several tools for risk profiling which are used to trace illicit funds for money laundering or terrorist acts (Levi & Wall, 2004; Amoore & de Goede, 2005; de Goede, 2008; Williams, 2013). These systems can analyze vast amounts of transactional data in real-time, identify suspicious patterns, and alert authorities or financial institutions for further investigation. An integrated analytical approach can be used in order to detect suspicious transactions, under the fraud alerts that contact the cardholder for approval (using various channels such as voice, email or SMS) in real time (Zoldi, 2015). Then, biometric authentication is another digital solution that can help prevent financial crimes. Biometrics refers to the

measurement and analysis of unique physical or behavioral characteristics of individuals, such as fingerprints, iris patterns, voiceprints, or facial features. These biometric traits are highly distinctive and difficult to forge or replicate, making them effective for identity verification.

Biometric authentication offers several advantages over traditional methods of authentication, such as passwords or PINs, which can be stolen, guessed, or forgotten. Despite its benefits, it's important to note that biometric authentication is not foolproof. Biometric data can still be stolen or compromised, and there are potential privacy concerns associated with its use. Therefore, it is crucial for financial institutions and organizations to implement robust security measures to protect biometric data and ensure its proper usage.

The latest development in blockchain technology is the fusion of blockchain with the most comprehensive possibilities of future cutting-edge technologies such as the Internet of Things, cloud computing, AI and robotics. The system can achieve unlimited scalability by exploring the potential of virtual blockchains within a single blockchain. This fusion is considered by many to be the latest generation of technology, Blockchain 4.0 [Garg, 2021]. Applying two common disruptive technologies, blockchain and Artificial Intelligence, to the field of decision reasoning is particularly exciting. The digital record of the blockchain provides insights into the framework behind AI and the source of the data it uses, thus addressing the challenge of explainable AI. The use of open-source blockchain solves the black box effect of AI, making the data output transparent. This will help improve confidence in the integrity of the data. Therefore, the recommendations AI can make increase consumer safety, and the use of blockchain to store and distribute AI models provides an audit trail, while pairing blockchain with AI can enhance data security.

On the other hand, AI can read, understand and correlate data at incredible speeds and comprehensively, bringing a new level of intelligence to blockchain-based business networks. By providing access to large amounts of data inside and outside the organization, blockchain helps AI scale to provide more actionable insights, manage data usage and model sharing, and create a reliable and transparent data economy. The combination of blockchain and AI can be particularly effective, fast and reliable when used with the Internet of Things (IoT). The IoT enables devices to send data over the internet to private blockchain networks to create tamper-proof records of common transactions. Open, interoperable, and multi-cloud blockchain allows business partners to share and access IoT data without central control and management. Each transaction can be verified to prevent disputes and build trust between all authorized network members.

Integrating IoT, AI and blockchain introduces a new system architecture that controls and improves most processes related to human well-being. This integration will have obvious implications for legal constructs, contracting and enforcement, data protection and consumer protection. This interconnection and integration of technologies have already appeared in market practice, including in the field of financial services. Again, practice is ahead of legal solutions, with applicable law, safeguards and liability law, appropriate redress systems, standards and protocols to be developed (Guergov and Radwan 2021).

Importance of human oversight, proper human oversight mechanisms must be put in place, and AI systems must support human autonomy and decision-making in which the human makes the final ruling. AI systems should provide partial or full outputs in formats easy to understand for the users and possibilities for interaction in an easy manner. It will be, therefore, of uttermost importance to further enhance approaches based on natural language processes and counterfactual explanations so as to help humans supervise and make meaningful decisions based on data outputs provided (Zanzotto, 2019); methods how to implement this so far have been domain-specific, based on current settings and scenarios in which the controller needs to supervise the AI-based solution.

Cyber education

Another important tool against cybercrime attacks which is found among the priorities of the European Commission consists in **cybercrime and** cybersecurity **education** of people, meaning how to use internet wisely and safely (Dalli, 2019). Through cyber education people should be empowered with knowledge on how to respond effectively to cyber-attacks (European Agency for Cybersecurity ENISA, 2022). The recent report of the European Agency for Cybersecurity (ENISA) from December 2022 titled "Cybersecurity Education Initiative on The EU Member States" aims to identify the needs and gaps regarding cybersecurity education and determine how ENISA can provide additional support to the Member States.

The recent report o ENISA (December 2022) shows the initiatives in cybersecurity education being carried out in the Member States, where it is observed that governments intend on introducing cybersecurity topics through the educational curriculum or training plans carried out in the school setting. Member States like Italy presented specific regional initiatives that will be carried out in additional regions in the future. Some Member States (40%) showed that non-governmental organization (NGOs) and institutions already involved in carrying out activities with children and adolescents have developed additional initiatives that present and

teach the principles of cybersecurity through more practical or engaging approaches such as events, competitions, online platforms, and games.

Another important type of preventive measure of digital fraud consists in the investments in anti-fraud programs / technologies by entities to prevent various types of frauds such as fraudulent insurance claims, identity theft, and money laundering. The market of these programs was estimated to be more than double in 2021 compared with 2017 and the projection for the market in 2023 exceeds 63 billion USD (Markets and Markets, 2021). An explanation regarding the high level of digital fraud undertaken in the context of increased IT technologies consists in the pace of technical enforcement ability to deal with these crimes (Gogolin, 2010). Digital skills are perishable unless kept current and thus digital crime investigation is very expensive. To keep the pace, digital crime investigation requires high investments in training and also digital and physical infrastructures (Gogolin, 2010).

However, not only the problem of cybercrime education is in our view, but problems have also persisted in the more general area of financial education. There are wide disparities regarding financial education in the EU Member States. The level of financial education highly differs among the EU countries. Thus, it is lower in countries from Southern Europe, i.e. Greece, Italy, and Portugal, but much higher in the Northern EU countries, such as Denmark, Sweden, the Netherlands, and Germany.

Financial regulation with technology

However, it is not only disruptive technologies that should and can be regulated, but new technologies also create opportunities to transform existing technologies and regulation itself. Whereas traditional regulation is based on (often imprecise and unenforceable) regulations and their ongoing accountability, and thus relies on large, centralized control organizations with human (subjective) resources, disruptive general-purpose technologies can ensure that socio-economic needs are met more quickly and reliably, based on a much wider range of patterns, by incorporating algorithmic safeguards.

New technologies can also work effectively in de-personalized (anonymized) data environments. Although there is no clear position on the interpretation of the concept of anonymization in the case law (hence the unpredictability of case law), national and supranational regulators have indicated that there may be alternatives to the total destruction of data that can ensure compliance with the GDPR. The Austrian DPA, for example, has acknowledged that it has flexibility on the technical means to achieve erasure and that

anonymization can be considered as one means to achieve erasure. Furthermore, the UK Information Commissioner's Office has long argued that if data are "rendered unusable", this may also be satisfactory. However, there does not seem to be consensus on this issue in all Member States (Finck, 2019).

Also, in line with Article 25 of the GDPR, developers of systems using Artificial Intelligence and blockchain technology are continuously working on developing (built-in) technical options to facilitate compliance with the GDPR. Each of these solutions entails important trade-offs, which will obviously vary depending on the context, and cannot be considered in general terms. These include, but are not limited to, zero proof of knowledge, the use of stealth addresses, homomorphic encryption, state channels for bilateral smart contracts, ring signatures, noise addition, chameleon hashes and editable blockchain, secure multi-agent computation, third-party indirection services, etc. It should be stressed that new developments specific to emerging new blockchains are constantly emerging, so their GDPR compliance also needs to be continuously assessed and updated (Finck. 2019). Regulation has for centuries been designed to apply to centralized entities (e.g. corporations) where hierarchies of control and responsibility are more easily identified. However, the fact that such structures are absent in decentralized environments does not in itself argue against regulating them. Rather, it is a matter of finding the right regulation rather than applying to a different environment a set of rules previously developed under different conditions.

4. Discussion, implications for policy, and the path forward

The previously highlighted characteristics of AI suggest that the potential large number of infringements affecting a wide range of consumers that may result from its use cannot be effectively remedied ex post under the current liability regime. In many cases, the developer and the user of the system are not able to detect the infringement and possible dysfunctional effects of the product in advance, even with the greatest care, and are consequently unable to inform the lay consumer of the risk of infringement.

To remedy this situation, the state must provide regulatory and professional assistance to bridge the current information asymmetry between the professional, but far from perfectly informed, service provider and the lay consumer. In supervisory activity, the characteristics of the service provider state must predominate over the role of the public authority. Supervision must focus on establishing and maintaining a balance in consumer protection, using a wide

range of instruments, of which fines are only one. On the one hand, systems using AI should be subject to strict rules and obligations on product safety and product liability before they enter the market, and to "consumer protection by design" along the lines of "privacy by design". On the other hand, public authorities should carry out a professionally controlled trial run with market players. Skilton and Hovsepian (2018) also stress the importance of continuous trials to avoid unintended effects.

The EU has also called for the creation of safety test tracks and exclusion zones for testing AI-based applications in the so-called Delvaux report (EP, 2019), and the principle of such testing is not unknown in practice. Such testing standards are for example included in the pharmaceutical industry regulations or in the Anglo-Saxon and Far Eastern rules for regulatory sandboxes, and the experience of this should be examined in detail and applied accordingly. A secondary effect of the use of sandboxes could be that supervisors gain direct experience of product development practices, developer thinking and objectives. Through cooperation developers also gain direct knowledge of consumer protection approaches, thus raising the level of financial literacy.

Auditing and enforcement of regulation is of big importance too, and it will be to see how this will unroll in the context of the EU, now that the AI Act is voted on and it's a reality. Enforcing is indeed the key and will drive commitment for companies. Yet another reflection for the path forward is that now there are probably too many regulations existing in the sphere of digital, all a little bit applicable, and this is overburdening companies, and the society. Now there are probably even too many digital laws, all a little bit applicable, and a good question is if further laws are needed, or the existing ones need to be made "crisper".

Enforcement of the AI Act may follow the GDPR enforcement strategy, that is that the EU installs offices in different locations, and thus acts and operates locally in the domain of competence. This enforcement may even try to fix from the experiences of implementing GDPR, fighting against bias, and processing of personal data for regulatory sandboxes, and these will have huge impacts on GDPR as well. Digital coordination platforms, in which different agencies work together may be the way forward in implementing AI regulation at countries level. Coordination between different bodies will be a key. However, it would seem useful to undertake a review in line with the policy principles set out in the Finck report to improve the GDPR in order to create legal certainty before moving offices, which would involve significant costs and administration. To this end, substantive coordination of supervisory bodies can be taken forward. The experience gained in regulatory sandboxes can

also greatly help to raise the professional standards of supervisors and to promote meaningful coordination.

In case of high-risk scenarios of application of AI in Finance, in general, and in cybercrime in particular, like we mention in this article, it may be handy to have specialized figures only on AI regulation aspects. These figures can work closely and together with data protection officers, to be sure of correct implementation of the AI Act. But Data Protection Officer would not be currently qualified to correctly interpret the requirements of the AI Act, and must be trained in addition, which is probably not ideal for companies. The approach should be to not multiply all such activities, as it will overwhelm people. New knowledge on how to structure the organizations internally for these challenges and implications is needed.

The Finck study (Finck, 2019), commissioned by the European Parliament immediately after the GDPR came into force, concluded that blockchain is not yet clearly regulated through the various elements of European data protection law and this could also apply to AI. He saw the reason for this in two overarching factors: first, that very often the technical architecture of blockchain technology itself, as well as its governance systems, are in conflict with the requirements of the GDPR. Second, the in-depth investigation revealed wider uncertainties in the legal framework, in the interpretation and application of the GDPR (e.g. the concepts of controller and processor, personal data or anonymization). The uncertain legal environment makes it difficult for data controllers to build appropriate and effective safeguards into the new technologies they deploy.

That said, the biggest challenge of the future will be to protect individuals from the risks of digital assets, including cybersecurity and hacker attacks, while enabling technological innovation. However, the systematic review also reveals that new technologies and data protection regulation are not irreconcilably at odds with each other, but that predictability and mutual adaptation are needed in this area, too. Indeed, they can be mutually supportive to each other's effective unfolding: the characteristics of AI and blockchain technology can also benefit the data economy more broadly, for example by facilitating the sharing of data between institutions to support data markets, which in turn can support the development of AI in the EU. On the other hand, the same features could also be used to support some of the objectives of the GDPR, such as giving data subjects more control over personal data that directly or indirectly concerns them (Finck, 2019).

The Finck report made three policy recommendations: first, it proposed the development of specific guidance on the application of the GDPR to blockchain technologies to ensure legal

certainty (note that interpretation of data protection provisions would be needed continuously as new technologies emerge and evolve, involving experts with knowledge of the technologies); second, it proposes to support codes of conduct and certification mechanisms to ensure that the principles of European data protection law are applied to the processing of personal data. This would also require meaningful dialogue and cooperation between data protection authorities and business experts. Thirdly, it suggests interdisciplinary research, technical and governance solutions and experimentation with protocols. The recent EU and national legislation to ensure the functioning of blockchain regulatory sandboxes could be an excellent tool for this purpose.

The most significant problem is the interpretation of data minimization, limited storage, purposeful processing and anonymization, as it is precisely in large-scale databases collected from different sources that technologies look for patterns that cannot be deleted in order to enhance human well-being (e.g., more reliable medical imaging, faster and more reliable services, etc.).

The challenges and questions that companies face require knowledge and expertise from different areas. To solve these challenges, a team must be formed with different roles. This team includes people who handle and organize data from various sources within the company, people who analyze the data and create reliable machine learning models, people who understand the company's business processes, people who ensure that decisions are made in accordance with regulations, and people who provide guidance on ethical criteria within the company's domain.

Finally, the EU is creating a digital finance platform called the European Commission's Digital Finance Platform. The goal of this platform is to bring together FinTech companies, banks, and regulators to encourage cooperation and creativity using financial data. The initial task was to create a map of the ecosystem. Currently, there are 9000 FinTech companies in Europe. Next, we needed to figure out what the different people using the platform needed and the situations in which they needed support. We found that everyone using the platform was interested in preventing fraud and managing risk. These actions will continue to spark conversations about how Artificial Intelligence can be used in this area.

5. Conclusions

This main goal of this work is to address the main issues that derive from the adoption of Financial Technologies (FinTech). We conduct a bibliometric and systematic literature review to assess the theoretical background present in the specialized literature, in a way that elucidates

the reasons for the topic's significance, ultimately revealing the research gap that this study intends to address. We have discussed important topics that have raised in relation with FinTech, such as the presentations of advantages and risks, the huge need for regulation, the need for financial inclusions, the increased risks given to the financial transactions and how to face these cybercrimes within potential solutions. We also explored how financial companies can use new technologies to create new services and products using the large amount of data they have. We have discussed the implications of our work for policy makers from different levels from the microeconomic, macroeconomic but also European level.

Further research will be needed to study the relation between new technology development, cybercrime, and societal harm. The idea that non-sentient machines make impactful societal decisions, therefore protecting and regulating new technologies to protect cybercrimes is an important issue to be addressed. In this paper we give our first analysis of the problems as well as important possible solutions at stake. Broader discussions will be needed, regarding the "good" vs "bad" side of new tech systems and how these are guiding the adoption of them. Additionally, how can efforts to educate people, on a mass scale, on the threats and opportunities posed by AI and on their individual rights in the face of these systems be best progressed? (Elliott, 2021). There may be the need for specific safety engineering frameworks for responsible AI as well.

How these different considerations will be interpreted into laws will require consideration of the dangers of new technologies against the potential for advancement that these new technologies hold. As financial domain policymakers combine these components in particular laws, the interests of the involved stakeholders must be considered as well.

The nature, level and applicability of regulation within the financial industry, will ought to adjust and combine, in our view, different interests, foremost societal, however also the interests of the involved stakeholders and entities (central banks, financial institutions and organization). The main principles of new tech and regulation in the domain will be around the pillars of accountability, trustworthiness, responsibility, and it is vital that regulators align different existing frameworks into a single consistent set of policies. With this they will also enhance innovation and improve competitiveness in the domain.

References

Achim, M.V., Borlea, N.S. & Văidean, V.L. (2021). Does technology matter for combating economic and financial crime? A panel data study, Technological and economic development of economy 27 (1), 223-261.

Barefoot, J.A., (2022). The case for placing AI at the heart of digitally robust financial regulation, Report, https://www.brookings.edu/research/the-case-for-placing-ai-at-the-heart-of-digitally-robust-financial-regulation/ (access on June 7, 2023).

Beaumont, P., Horsburgh, B., Pilgerstorfer, P., Droth, A., Oentaryo, R., Ler, S., Nguyen, H., Ferreira, G. A., Patel, Z., & Leong, W. (2021). CausalNex [Computer software]. https://github.com/quantumblacklabs/causalnex

Bellamy, R. K., Dey, K., Hind, M., Hoffman, S. C., Houde, S., Kannan, K. & Zhang, Y. (2018). AI Fairness 360: An extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias. *arXiv preprint arXiv:1810.01943*.

Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C., Konecny, J., Mazzocchi, S., McMahan, B. & Roselander, J. (2019). Towards federated learning at scale: System design. *Proceedings of machine learning and systems*, *1*, 374-388.

Bresnahan, T. F., & Trajtenberg, M. (1995). General purpose technologies 'Engines of growth'?. *Journal of Econometrics*, *65*(1), 83-108.

Broniatowski, D. A. (2021). Psychological foundations of explainability and interpretability in artificial intelligence. *NIST, Tech. Rep*.

Budai, B.B. (2008). E-Public Administration in an Axiomatic Approach, Ph.D. thesis, Pécs 2008.https://ajk.pte.hu/files/file/doktori-iskola/budai-balazs-benjamin/budai-balazs-benjamin-vedes-ertekezes.pdf

Chamorro-Premuzic, T., Polli, F., & Dattner, B. (2019). Building ethical AI for talent management. *Harvard Business Review*, *21*, 1-15.

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS quarterly*, 1165-1188.

Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review*, *4*(1), 79-90.

Coita, I.F., Belbe, S., Mare, C., Osterrieder, J., & Hopp, C. (2023a). Modelling taxpayers' behaviour based on prediction of trust using sentiment analysis. *Finance Research Letters*, *58*(Part C), 104549.

Coita, I.F., Iannario, M., Iodice D'Enza, A., & Mare, C. (2023b). Modelling the assessment of taxpayer perception on the fiscal system by a hybrid approach for the analysis of challenging data structures. *Digital Finance* (2023). https://doi.org/10.1007/s42521-023-00092-y.

Cooper, et al. (2022), "Accountability in an algorithmic society: relationality, responsibility, and robustness in machine learning.," in ACM Conference on Fairness, Accountability, and Transparency, Seoul, South Korea, 2022.

Cortet, M., Rijks, T., & Nijland, S. (2016). PSD2: The digital transformation accelerator for banks. *Journal of Payments Strategy & Systems*, *10*(1), 13-27.

Cummings, R., Desfontaines, D., Evans, D., Geambasu, R., Jagielski, M., Huang, Y., ... & Zhang, W. (2023). Challenges towards the Next Frontier in Privacy. *arXiv preprint arXiv:2304.06929*.

Devlin, J. F., Ennew, C. T., Sekhon, H. S., & Roy, S. K. (2015). Trust in financial services: Retrospect and prospect. *Journal of Financial Services Marketing*, *20*, 234-245.

Dimitropoulos, Georgios: The Law of Blockchain, 95 Wash. L. Rev. 1117 (2020). Available at: https://digitalcommons.law.uw.edu/wlr/vol95/iss3/3

Edemman (2019). 19th Annual Trust barometer : Financial Servicies, available at : https://www.edelman.com/research/2019-artificial-intelligence-survey

Elliott, K., Price, R., Shaw, P., Spiliotopoulos, T., Ng, M., Coopamootoo, K., & van Moorsel, A. (2021). Towards an equitable digital society: artificial intelligence (AI) and corporate digital responsibility (CDR). *Society*, *58*(3), 179-188.

Ellul, J. (2022). Should we regulate Artificial Intelligence or some uses of software?. *Discover Artificial Intelligence*, *2*(1), 5.

Eszteri, D. (2020). On the GDPR-compliance of blockchain as a personal data management technology, *State and Law, LXI 4(4),* 24 - 51 http://real.mtak.hu/118513/1/2020-04_ESZTERI-tan.pdf

European Commission (2019). High-level expert group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, European Commission. European Commission (2000). Charter of fundamental rights of the European Union, Official Journal of the European Communities, 364(1), 1–21

European Commision (2018). "General Data Protection Regulation - GDPR," Brussels, 2018.

European Commission, Digital finance platform, https://digital-finance-platform.ec.europa.eu/

European Union (2021). European Union Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act, AI Act) and amending certain Union Legislative Acts. COM/2021/206 final.

European Parliament (2022). "The Dutch childcare benefit scandal, institutional racism and algorithms," 28 June 2022. [Online]. Available: https://www.europarl.europa.eu/doceo/document/O-9-2022-000028_EN.html#def1.

European Parliament, REPORT with recommendations to the Commission on Civil Law Rules on Robotics, https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html

Finck, M. (2019). „Blockchain and the General Data Protection Regulation" Can distributed ledgers be squared with European data protection law? *European Parliamentary Research Service*, PE 634.445, July 2019, 33.

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Garg, R. (2021). *Blockchain for Real World Applications*, ISBN: 9781119903734.

Guergov, S., & Radwan, N. (2021). Blockchain convergence: Analysis of issues affecting IoT, AI and blockchain. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *1*(1).

Hamon, R., Junklewitz, H., & Sanchez, I. (2020). Robustness and explainability of artificial intelligence. *Publications Office of the European Union*, *207*.

Hauer, T. (2018). Society and the second age of machines: Algorithms versus ethics. *Society*, *55*, 100-106.

Hauer, T. (2022). Importance and limitations of AI ethics in contemporary society. *Humanities and Social Sciences Communications*, *9*(1), 1-8.

IBM Corporation (2022). IBM Global AI Adoption Index 2022. May. United States of America.

Jagtiani, J., & Lemieux, C. (2019). The roles of alternative data and machine learning in fintech lending: evidence from the LendingClub consumer platform. *Financial Management*, *48*(4), 1009-1029.

Jain, S., Luthra, M., Sharma, S., & Fatima, M. (2020). Trustworthiness of artificial intelligence. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 907-912). IEEE.

Kelley, S., Ovchinnikov, A., Hardoon, D., & Heinrich, A. (2021). Anti-discrimination Laws, AI, and Gender Bias: A Case Study in Non-mortgage FinTech Lending, Manufacturing & *Service Operations Management* 0(0), https://doi.org/10.1287/msom.2022.1108

Khera, P., Ogawa, S., Sahay, R., & Vasishth, M. (2022). Women in Fintech: As Leaders and Users.

Kherbouche, M., Pisoni, G., & Molnár, B. (2022). Model to program and blockchain approaches for business processes and workflows in finance. *Applied System Innovation*, *5*(1), 10.

Kiron, D., & Schrage, M. (2019). Strategy for and with AI. MIT Sloan Management Review, 60(4), 30–35

Koshiyama, A., Kazim, E., Treleaven, P., Rai, P., Szpruch, L., Pavey, G., ... & Lomas, E. (2021). Towards algorithm auditing: a survey on managing legal, ethical and technological risks of AI, ML and associated algorithms.

Koulu, R. (2020). Proceduralizing control and discretion: Human oversight in artificial intelligence policy, *Maastricht Journal of European and Comparative Law*, 27(6), pp. 720-735, 2020.

Krafft, P. M., Young, M., Katell, M., Lee, J. E., Narayan, S., Epstein, M., ... & Barghouti, B. (2021). An action-oriented AI policy toolkit for technology audits by community advocates

and activists. In *Proceedings of the 2021 ACM conference on fairness, accountability, and transparency* (pp. 772-781).

Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?. *International journal of law and information technology*, *26*(1), 45-63.

Lipsey, R. G., Carlaw, K. I., & Bekar, C. T. (2005). *Economic transformations: general purpose technologies and long-term economic growth*. Oup Oxford.

Lipton, Z. C. (2018). The mythos of model interpretability: In machine learning, the concept of interpretability is both important and slippery. *Queue*, *16*(3), 31-57.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, *122*, 875-888.

Lukyanenko, R., Castellanos, A., Parsons, J., Chiarini Tremblay, M., & Storey, V. C. (2019). Using conceptual modeling to support machine learning. In *Information Systems Engineering in Responsible Information Systems: CAiSE Forum 2019, Rome, Italy, June 3–7, 2019, Proceedings 31* (pp. 170-181). Springer International Publishing.

Lukyanenko, R., Castellanos, A., Samuel, B. M., Tremblay, M. C., & Maass, W. (2021). Research Agenda for Basic Explainable AI. In *AMCIS*.

Lukyanenko, R., Maass, W., & Storey, V. C. (2022). Trust in artificial intelligence: From a Foundational Trust Framework to emerging research opportunities. *Electronic Markets*, 1-28.

Maia, G., & Vieira dos Santos, J. (2021). MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and'Decentralised Finance'). *Forthcoming article in" Blockchain and the law: dynamics and dogmatism, current and future*.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys (CSUR)*, *54*(6), 1-35.

Mihale-Wilson, C., Hinz, O., van der Aalst, W., & Weinhardt, C. (2022). Corporate digital responsibility: relevance and opportunities for business and information systems engineering. *Business & Information Systems Engineering*, *64*(2), 127-132.

Miller, T. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial intelligence*, *267*, 1-38.

Misheva, B. H., Osterrieder, J., Hirsa, A., Kulkarni, O., & Lin, S. F. (2021). Explainable AI in credit risk management. *arXiv preprint arXiv:2103.00949*.

Monarch, R. M. (2021). *Human-in-the-Loop Machine Learning: Active learning and annotation for human-centered AI*. Simon and Schuster.

Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011). Can homomorphic encryption be practical?. In *Proceedings of the 3rd ACM workshop on Cloud computing security workshop* (pp. 113-124).

Narayanan, M., Chen, E., He, J., Kim, B., Gershman, S., & Doshi-Velez, F. (2018). How do humans understand explanations from machine learning systems? an evaluation of the human-interpretability of explanation. *arXiv preprint arXiv:1802.00682*.

Novelli, C., Taddeo, M., & Floridi, L. (2023). Accountability in artificial intelligence: what it is and how it works. *AI & SOCIETY*, 1-12.

OECD, (2021). Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers, https://www.oecd.org/finance/artificial-intelligence-machine-learningbig-data-in-finance.htm

Pedersen, N. (2020). *Financial technology: case studies in FinTech innovation*. Kogan Page Publishers.

Pisoni, G. (2020). Going digital: Case study of an Italian insurance company. *Journal of Business Strategy, 42(2)*, 106-115.

Pisoni, G., Molnár, B., & Tarcsi, Á. (2021). Data Science for Finance: Best-Suited Methods and Enterprise Architectures. *Applied System Innovation*, *4*(3), 69.

Pisoni, G., & Díaz-Rodríguez, N. (2023). Responsible and human centric AI-based insurance advisors. *Information Processing & Management*, *60*(3), 103273.

REGULATION (EU) No 2022/858 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on a pilot scheme for market infrastructures based on shared ledger technology and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A32022R0858

Rosenblatt, E. (2020). *Credit data and scoring: the first triumph of big data and big algorithms*. Academic Press.

Saleiro, P., Kuester, B., Hinkson, L., London, J., Stevens, A., Anisfeld, A., ... & Ghani, R. (2018). Aequitas: A bias and fairness audit toolkit. *arXiv preprint arXiv:1811.05577*.

Scheau, M. C., Crăciunescu, S. L., Brici, I., & Achim, M. V. (2020). A cryptocurrency spectrum short analysis. *Journal of Risk and Financial Management*, *13*(8), 184.

Schumpeter, J.A. (1911) The Theory of Economic Development. Harvard University Press, Cambridge.

Schwab, Klaus: Four leadership principles for the Fourth Industrial Revolution, https://www.weforum.org/agenda/2016/10/four-leadership-principles-for-the-fourth-industrial-revolution/

Sharma, S., Henderson, J., & Ghosh, J. (2020). CERTIFAI: A common framework to provide explanations and analyse the fairness and robustness of black-box models. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (pp. 166-172).

Shaw, P., Hervey, M., & Lavy, M. (2021). Context Matters": The Law, Ethics and AI. *Hervey, M., and Lavy, M. The Law of Artificial Intelligence, Croydon: Sweet & Maxwell (Thomas Reuters), CPI Group, UK*, 31-66.

Shneiderman, B. (2022). *Human-centered AI*, Oxford University Press.

Silberg, J., & Manyika, J. (2019). Notes from the AI frontier: Tackling bias in AI (and in humans). *McKinsey Global Institute*, *1*(6).

Skilton, M., & Hovsepian, F. (2018). *The 4th Industrial Revolution, Responding to the Impact of Artificial Intelligence on Business,* Palgrave Macmillan, https://doi.org/10.1007/978-3-319-62479-2

Sohangir, S., Wang, D., Pomeranets, A., & Khoshgoftaar, T. M. (2018). Big Data: Deep Learning for financial sentiment analysis. *Journal of Big Data*, *5*(1), 1-25.

Sokol, K., Santos-Rodriguez, R., & Flach, P. (2022). FAT Forensics: A Python toolbox for algorithmic fairness, accountability and transparency. *Software Impacts*, *14*, 100406.

Thaler, R.M. (2017). *On what tree does behavioral economics grow?* - A video presentation by Richard M. Thaler. Hungarian Academy of Sciences.

Thaler, R.M. (2016). *Order-breakers - The rise of behavioral economics*. HVG Books, Budapest.

Tilson, D., Lyytinen, K. & Sørensen, C. (2010), Research commentary—digital infrastructures: The missing is research agenda, *Information systems research* 21(4), 748–759.

Tiwana, A., Konsynski, B. & Bush, A. A. (2010). Research commentary—platform evolution: Coevolution of platform architecture, governance, and environmental dynamics, *Information systems research* 21(4), 675–687.

Truby, J., Brown, R., & Dahdal, A. (2020). Banking on AI: mandating a proactive approach to AI regulation in the financial sector. *Law and Financial Markets Review*, *14*(2), 110-120.

Varshney, K. R. (2019). Trustworthy machine learning and artificial intelligence. *XRDS: Crossroads, The ACM Magazine for Students*, *25*(3), 26-29.

World Bank Group, (2022). *Smart Contract Technology and Financial Inclusion*. FinTech Note; No. 6. World Bank, Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/33723 License: CC BY 3.0 IGO.

Xiong, P., Zhu, T., & Wang, X. F. (2014). A survey on differential privacy and applications.

Yang, J., Zhou, K., Li, Y., & Liu, Z. (2021). Generalized out-of-distribution detection: A survey. *arXiv preprint arXiv:2110.11334*.

Yoke Wang T., Heng, D. (2022). *FinTech: Financial Inclusion or Exclusion*? IMF Working Paper no. WP/2022/080.

Zanzotto, F. M. (2019). Human-in-the-loop artificial intelligence. *Journal of Artificial Intelligence Research*, *64*, 243-252.