

Tomasz Nieborak

Adam Mickiewicz University, Poznań, Poland

tomasz.nieborak@amu.edu.pl

ORCID ID: 0000-0002-5499-9353

Digital Coercion? The Financial Market and the Right to Digital Opt-Out between Fiction and Reality

Abstract: This article examines the challenges that digitalisation poses for the regulation of contemporary financial markets and the implications for individual freedom. The financial sector demonstrates how 'digital coercion' can threaten the right not to use technology, raising questions about the balance between protecting citizens' rights and enabling participation in a digitalised economy. The focus is on how technological development, especially artificial intelligence (AI), affects everyday interactions with financial systems and whether individuals still have a genuine choice to remain outside digital frameworks. The analysis relies primarily on the dogmatic-legal method, complemented by axiological reflection and critical legal perspectives, to reveal tensions between existing regulations, constitutional values and human rights. Digital coercion occurs when opting out of technology is no longer practically possible, particularly in finance where alternatives diminish as digital tools dominate. While it may be theoretically possible to avoid financial technology, doing so risks exclusion from essential functions such as accessing credit or managing finances. EU regulations like the AI Act, MiCA and DORA reinforce this process, promoting and effectively enforcing digitalisation while limiting the right to digital opt-out. Although these frameworks aim to safeguard privacy and freedom, in practice technologies and algorithms increasingly shape financial markets, often in opaque ways. In line with Lawrence Lessig's notion that 'code is law', algorithms become de facto lawmakers, establishing norms that constrain free consumer choice. Consequently, the right not to use technology becomes largely illusory when access to fundamental services depends on technological infrastructure.

Keywords: financial market regulation, right to digital opt-out, financial exclusion, human rights, European Union, FinTech, Decentralised Finance, human beings

Introduction

It will soon be 100 years since the publication of the novel *Brave new world* by Aldous Huxley (1946). The novel combines elements of both prophetic vision and warning. Reading it today, in the age of technological revolution and ongoing debates about the future role of artificial intelligence (AI) in our daily lives, it takes on a completely different dimension (Boden, 2020, pp. 96–113). For we are now facing the emergence of a new world – Huxley’s World State – which is linked through complex IT systems that operate on the basis of increasingly sophisticated and self-learning computer technologies. These systems affect all the major spheres of our everyday lives. Although this reality is a human creation, there is growing concern about the potential for these technologies to take control of our lives and, as it were, create a social destiny which will be accepted by society, much like in the *Brave New World* – a society where most men and women will grow up to love their servitude and will never dream of revolution (Huxley, 1946, pp. xvi–xvii), in exchange for comfort and everyday stability. Today, nearly a century later, Huxley’s warning seems uncannily relevant, particularly in the context of digital coercion, which is no longer optional but rather the default mode of operation for the human being in the realm of services, including financial services. At times it may even seem that the individual, a consumer in the financial market, although seemingly aware and informed (Cyman, 2023, pp. 55–56), has become just another cog in the financial system, a system in which AI increasingly plays, and will continue to play, a pivotal role. But will this lead to a situation where autonomous IT systems effectively take over the governance of our reality, including the financial one? A reality of Huxley’s World State, structured to ensure that ‘when the individual feels, the community reels’ (Huxley, 1946, p. 110)?

While this dystopian vision of society is terrifying, it is not entirely unrealistic. It prompts us to ask questions about possible alternatives, such as, for instance, a world in which humans can control the extent to which technology interferes in their daily lives (Stacewicz, 2023). This would be a world akin to Huxley’s ‘Savage Reservation’, governed by old, ‘natural’ rules, rejecting the new order. One must then ask: Is the right not to use digital technologies, and its protection by law or other regulatory means, still possible – or has it already become an anachronism in the digital dogma of modernity? Or is it already becoming an anachronism in the digital dogma of modernity, even more so when the subject of study is the financial market and its legal regulation, the identification of which, it turns out, presents another research problem? Another question that arises in view of the above is whether the technological revolution has led to a situation in which new, self-creating sources of financial market law are hidden in algorithms created by hidden lawmakers who use self-learning algorithms to adjust relevant systems and rules on an ongoing basis, based on changing market conditions.

In view of this, is it true that, as Lawrence Lessig wrote, 'code is law' (1999, p. 3)? The search for an answer to this question is the central theme of this article, contained in this issue of *Białystok Legal Studies* devoted to the non-use of digital technologies and the protection of such non-use by law as well as by other means of regulation. As editor Elżbieta Kuźelewska rightly observes: 'As the contemporary ubiquity of new technologies leaves little if no choice for individuals whether to use them, our interest in legal and other regulatory means to protect their non-use merits both academic and professional attention' (Kuźelewska, 2025).

One of the key areas requiring attention in this regard is the financial market, the rules and operational architecture of which have undergone revolutionary changes in recent years. This is largely due to the widespread adoption of AI by FinTech players, who have successfully challenged traditional market operators – particularly banks – by offering consumers attractive, affordable financial solutions based on modern technology. However, embedded in the 'genotype' of these products is a coercion to use new technologies. While opting out is theoretically possible, in the long term it results in exclusion from access to the one resource crucial for life which is money (Kowalewska & Musiał, 2025). Money is essential for securing daily needs as well as for personal self-realisation, such as acquiring material goods or achieving a certain level of prosperity.

One could argue at this point that certain areas of financial market participation are becoming spaces where formal individual freedom (including human rights) does not translate into actual freedom of choice. Moreover, even though lawmakers strive to protect this freedom, the rules of the virtual reality system cause individuals to remain largely unaware of the mechanisms (algorithms) that track and then analyse their behaviour, and in certain situations influence their choices (Szozzkiewicz & Świergiel, 2018).

Naturally, no one is forced to use particular technological solutions. However, the modalities described by Lessig (law, markets, social norms or code) effectively eliminate the option of not using them. Who, then, is the true creator of our reality: the lawmaker or the code (algorithm)? Can this brave new world of modern financial markets be controlled in such a way that consumers have a genuine right of non-use, and will it be a right to choose an alternative, to enjoy transparency of operations and to exercise the choice of a non-algorithmic service, for example? And will such regulation, if adopted, be effective and efficient?

Even without prejudging the answers to these questions, it is already apparent at this point that it would be hard to imagine a contemporary financial market functioning without access to technology. This is also due to the actions of lawmakers (e.g. the EU), who, while trying to regulate this reality, in practice confirm the thesis of the actual absence of the possibility of guaranteeing a formal right to not use technology. As a result, current EU financial market regulations structurally exclude individuals who wish to function outside the digital infrastructure.

There are at least a few examples of this, and they include the fundamental EU financial market regulations such as the AI Act (2024), DORA (2022), MiCA (2023), PSD 2 (2015) and FIDA (2023). These legislative acts are too specialised and extensive to analyse in detail within the scope of this article, although selected examples will be used to support the main arguments formulated here. These include the assertions that 'digital coercion' exists in the EU financial market today and that the role of AI in creating and enforcing law is growing. This law may increasingly be a technical implementation of an algorithm. But who will write this algorithm: a human being or AI?

1. The financial market in the face of a new regulatory paradigm in the age of FinTech

For decades, financial markets have been based on the principle of stability and predictability. The traditional structures and divisions of the financial markets, the roles ascribed to them and, last but not least, the actors operating within them, banks in particular (commonly perceived as institutions of public trust), have remained constant. But 2008 brought the financial crisis that has been permanently etched into the pages of history as exceptional, not least because of its global nature and above all because of the underlying causes that led to it. Among these was the widespread use of financial derivatives as an investment strategy designed to generate additional profits, especially for banks (Jurkowska-Zeidler, 2008, p. 72). These profits were obtained through risk-trading mechanisms and the use for this purpose of funds entrusted to the financial sector by trusting clients. The outcome of this experiment is well known; one of its effects was the loss of that public trust and the consequent search for alternatives (Jurkowska-Zeidler, 2011). Although the conditions for the provision of new alternatives had been developing for years, this was precisely the moment for them to materialise in the form of the growth of the FinTech sector, supported by the dynamic development of AI.

Drawing on the ideas of Zygmunt Bauman (2006), one could argue that after 2008 the world witnessed the true face of 'liquid modernity', in which social structures, relationships, or values and identities are no longer stable or unchangeable, and a sense of security is eroding. Volatility and unpredictability are also features that characterise modern technology; it is evolving at a tremendous pace and in a direction that is nowadays difficult to foresee (Armour et al., 2016). This is an even greater challenge for lawmakers today, who are guided by the essence of the law and seek to frame this new reality within a legal framework, given the nature of modern technology, especially AI, and its ability to adapt and self-learn. But is this really possible? Or should lawmakers today not aim at fully controlling and shaping reality with the aid of traditional sources of law, as well as with the use of soft forms of regulation? Such soft law approaches are already being successfully used in the European Union's fi-

financial market regulation, one example being the Binding Technical Standards (Fedorowicz, 2021b).

Another challenge for modern legislatures in this context is the speed of change and the process of economisation of the law (Nieborak, 2016, pp. 75–94). Just as money has evolved from gold coins to virtual cryptocurrencies, AI will also evolve in ways that will affect our lives in a manner that we cannot fully foresee today. Yet the evolution of money spanned centuries, and the development of AI is measured in years. It can certainly be argued that it began as early as the 1950s with the publication of Alan Turing's essay 'Computing machinery and intelligence', but it was only in 2012 that the introduction of the AlexNet model demonstrated the power and potential of the new technologies (Krizhevsky et al., 2017). Around the same time, startups that today are icons of the FinTech sector, such as PayPal, Revolut and Square, began operating. Without their pioneering efforts, further progress in the areas of cryptocurrencies, neobanks like Monzo, InsureTech like Lemonade, or more recently RegTech (Nowakowski, 2020, pp. 13–56) would likely not have been possible. All of these innovations fall under the FinTech category. They are also a perfect example of the progressive process of financialisation, i.e. the penetration of the financial sphere into the real world and its impact on everyday life, through technological innovations (including AI) whose rules of operation are often only understood by a narrow group of specialists (so-called rocket scientists).

Among other things legislatures and supervisors are concerned about the significance of this area of the financial market for the socio-political situation, particularly with regard to protecting the interests of weaker actors (financial market consumers). Having previously fallen victim to the unethical actions of financial market players so far, in the new world they may now be subjected to forces created by a virtual reality based on algorithms used to analyse data and automate processes, as well as to assess their creditworthiness or examine their purchasing habits (Rutkowska-Tomaszewska, 2020). Consequently, in order to obtain a loan, authenticate personal data or confirm a transfer order, it becomes necessary to use digital technologies. This may be termed 'digital coercion', i.e. a situation in which the consumer is compelled to use digital solutions, even unwillingly, which clearly contradicts the idea of the non-use of digital services (Rutkowska-Tomaszewska & Gałązka, 2024). As a result, new technologies, especially those based on AI, are beginning to shape social norms significantly. These norms, alongside law, constitute a fundamental instrument for creating the reality around us.

The confrontation of these two entities, namely AI and the law, triggers a series of questions and doubts, the analysis of which, in my view, requires going back to the sources, i.e. answering the question about the essence of law. Relevant in this respect are the questions posed by Marek Smolak: How does law connect with the world? Is the legal system autonomous from its surrounding reality? Should it be understood merely instrumentally, as a means of achieving important non-legal objectives, including so-

cial, political and economic ones? (Smolak, 2001). However, given the complexity and speed of change in the world around us, as well as the impact on our daily lives, one has to agree with Włodzimierz Gromski's (2007, p. 51) thesis that it is also necessary to look at the law in its real aspect, as a factor shaping the attitudes and behaviours of members of society in accordance with models established or recognised by the state (the legislature). Law as a social phenomenon, therefore combining both the real and the formal aspects, is desirable, as it allows a holistic view of the reality around us. This becomes particularly relevant today, in the age of modern technology, when humanity's challenge is to find the right legal framework to ensure technological development on the one hand and human control over it on the other. This is particularly true of AI, the progress of which will surely only continue to move towards previously unknown forms (such as neural networks), transforming all aspects of our daily lives and work, as well as the functioning of the financial market, the essence of which lies primarily in the role it plays in the creation of what has always been the most important commodity – money. Money is the building block of capital, without which it would be difficult to imagine the functioning of the world and its development.

The birthplace of money is the financial market, where the revolution mentioned earlier, of which AI is one of the protagonists, is taking place. The sources of this revolution should be sought in the change in the approach of lawmakers, including EU legislatures, and their attempts to regulate this segment of the market. This new approach manifests itself in disintermediation and the growing role of new types of financial intermediaries, among other things, for which legislatures alone are opening the door. One example is the EU regulation of the payment services market; crucial in this respect is the Payment Services Directive 2 (Zalcewicz, 2016), which in the name of increasing market competitiveness allowed so-called Third Party Providers (TPPs) access to the market, seen as an example of the open banking concept (Masłowski, 2024, pp. 20–50). Using cutting-edge technological solutions, TPPs often sense upcoming trends in advance and offer a range of innovative instruments that are often faster and easier to operate. This has obviously contributed to their appeal to customers, even though consumers are not always aware of how these mechanisms work. Depending on the type of TPP in question, i.e. an Account Information Service Provider or a Payment Initiation Service Provider, and with the consumer's consent, opportunities then arise for the provider of a given service to access valuable data, such as the user's account information (transaction history, balance) or personal finance management behaviour, or the ability of the provider to initiate certain transactions directly from the user's bank account, which always require the user's authorisation (Szpringer & Szpringer, 2014).

As can be seen, although the specific role of the human being is taken into account in these processes, the secondary nature of the situation, related to the process of collecting and processing huge amounts of data – Big Data – is concealed (Szożkiewicz, 2021, pp. 33–46). Properly processed, structured and analysed in a spe-

cific context, these data constitute an excellent source of information, which, as Jean Baudrillard has rightly observed, is a form of control (Ziętek, 2013). Whoever has access to data has power over information and how it is used (Kusak, 2022). In the case of the data collected and processed in the financial markets, this power is immense and must be controlled. And yet as the nature of AI evolves towards more rapid self-learning and AI adaptation, are we not going to be faced with a situation where any attempt to regulate this entity becomes merely an illusion of control? Exercising the right not to use digital technology may constitute a guarantee of individual freedom from digital coercion.

However, one must also be aware of the other side of this right, related to the potential exclusion and social marginalisation of people who refuse to accept algorithmic interference in their lives. Is it therefore possible to design an optimal system based on the values that are accepted and upheld in a given society? The debate on regulating AI is essentially a debate about values, not legal rules, and the ultimate shape of legal regulation depends on which values the lawmakers choose to prioritise (Jędrzejczak, 2024). But does the choice of values allow a situation where people are coerced to use the internet to exercise their rights or fulfil their duties (Kloza et al., 2025, p. 1)? What happens when the algorithm code becomes the actual, albeit hidden, legislation? The conditions currently created by the 'traditional' EU legislation to regulate the financial market actually aimed at supporting the development of the digital sector, and may soon, in my view, necessitate a redefinition of the paradigm of financial market regulation. The existing assumptions, theories, methods and values behind it either will be blurred or will require redefinition in the face of the emergence of a 'new' legislature and the acceptance of a new paradigm, namely that code is law, while the rules enshrined in this code will become a real regulatory force, a fourth modality of regulation, shaping entire societies whose spheres of activity will also be determined by it (Lessig, 1999, pp. 85–99). And all this in the age of a culture of immediacy and risk.

2. Is code law? Do new self-creating sources of financial market law already exist?

The answer to the question of whether code is law should begin with a brief description of the financial market, undoubtedly one of the most important spheres in which societies exist and function today (Bybee, 2016, pp. 21–23). The phenomenon of financialisation, whereby the financial sphere penetrates the real sphere and thus everyday life, aptly captures its importance (Engelen, 2008). To define financialisation we only need to reflect on our daily activities. The financial market permeates our lives in a number of ways: when we withdraw cash from an ATM, pay for purchases, buy insurance, go on holiday or take out a loan to finance the purchase of a house. These ac-

tivities are accompanied by a world that exists in parallel but is practically unknown to those who use services such as clearing and settling payments, credit and risk assessments, scoring or new financial instruments that are frequently based on the principle of freedom of contract between the parties (over-the-counter instruments). All of this poses a real challenge to market regulators, and the relevant processes are supported by modern technologies developed by sectors such as FinTech and significantly influence consumer behaviour, particularly in terms of capital management and interaction with financial institutions (Nowakowski, 2023, pp. 161–169). Mobile applications, the use of AI and the introduction of virtual trading platforms result on the one hand in growing automation that allows business transactions to be conducted from anywhere across the globe, but on the other hand they bring about digital coercion. This is naturally followed by a re-evaluation of traditional social norms related to privacy and transparency. Indeed, one might get the impression that consumers are willing to sacrifice their privacy, hitherto considered to be an absolute value, for convenience, speed and personalisation of services. The value of privacy is protected by the Universal Declaration of Human Rights, Article 12, which states that ‘no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks’ (United Nations, 1948). Does this new reality of the way financial markets operate pose a threat to this right? Can algorithms arbitrarily violate it? These questions must be asked by their creators, who, we assume, are always humans, who construct solutions based on a controlled version of AI, otherwise known as narrow AI (Footer, 2020).

While artificial general intelligence, considered to be the highest potential level of AI development, is currently only hypothetical, one might wonder whether it may become another ‘black swan’, a species that we are breeding which will eventually outperform us and which will, at some point, begin to compete with humans in terms of general reasoning, learning, problem-solving and the use of consciousness (Chłopecki, 2018, pp. 5–6). It might, for example, aim to control the financial system of which the financial market and its various components are a part. The financial market must be viewed in the broader context of the economic system, which is in turn part of the social system. While this may seem an obvious point, it is nevertheless of great importance and should serve as a guideline for lawmakers and those who apply their legislation. This interdependence means that any turbulence in the financial system will have specific consequences for the economy and consequently for society.

The EU legislature seems to understand this interdependence, as it successively includes new spheres of financial market operations within digital finance in its legal framework, simultaneously examining potentially necessary measures to be undertaken in areas such as crypto-assets, cyber-resilience, financial data access and the digital euro. The definition of ‘digital finance’ that may be found on one of the websites of the European Commission dedicated to this issue reads that it is ‘the term

used to describe the impact of new technologies on the financial services industry, which includes a variety of products, applications, processes and business models that have transformed the traditional way of providing banking and financial services'. We read further that:

while technological innovation in finance is not new, investment in new technologies has substantially increased in recent years and the pace of innovation is exponential. We now interact with our bank using mobile technology. We make payments, transfer money and make investments using a variety of new tools that were not there a few years ago. Artificial intelligence, social networks, machine learning, mobile applications, distributed ledger technology, cloud computing and big data analytics have given rise to new services and business models by established financial institutions and new market entrants. All these technologies can benefit both consumers and companies by enabling greater access to financial services, offering wider choice and increasing efficiency of operations. They can also contribute to bringing down national barriers and spurring competition in areas such as: online banking, online payment and transfer services, peer-to-peer lending, personal investment advice and services. The financial services industry has been influenced by innovative technology, which can benefit both consumers and companies by giving a greater access to financial services, offering wider choice and increasing efficiency of operations. Numerous opportunities involve also risks and challenges, which require monitoring and regulation. Therefore, the Commission has put further many initiatives to embrace the innovations, preserve market stability and integrity, and protect financial investors as well as consumers (European Commission, *Overview of digital finance*).

Aware of the changes taking place and the growing importance of AI in the financial market, on 24 June 2024 the European Union launched a targeted consultation on artificial intelligence in the financial sector. For that purpose, the Commission drew up a consultation document entitled 'Artificial intelligence in the financial sector' (European Commission, 2024), which contains numerous questions broken down by specific sectors of the financial market. It also highlighted that the targeted consultation will answer the questions posed in the document, divided into three parts: one with general questions on the development of AI, one consisting of questions related to specific use cases in finance and one on the AI Act as related to the financial sector. At the same time it was agreed that in the description of the purpose of the targeted consultation, the concept of AI corresponds to the definition of an AI system established in Article 3(1) of the AI Act 2024 and covers 'any machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it

receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments’.

The consultation period is now closed, and a summary, expected in the near future, will provide a valuable insight into the perception of AI by market participants in a broad sense, who have already been covered by regulations directly or indirectly applied pursuant to the AI Act. This Act, an extremely detailed and extensive regulation, introduces four types of AI and identifies them according to the degree of risk associated with their application:

- minimal-risk systems, which pose no significant security or human rights risks (e.g. spam filters),
- limited-risk systems, which affect the user, but create no serious risks (e.g. recommendations on e-commerce platforms),
- high-risk systems, the AI systems that pose a risk of harm to health and safety or an adverse impact on fundamental rights, which includes, among other things, credit risk assessments,
- unacceptable-risk systems, which are banned in the EU (with some exceptions related to the threat of terrorism) and which are regarded as contrary to the EU’s values, infringing fundamental rights. Among them are the ability to recognise emotions in a specific context and the social scoring system already in use in some countries to assess citizens, based on their behaviour, actions or characteristics.

The first two types of AI can be implemented without any additional compliance requirements. In contrast, high-risk systems must comply with certain requirements, including a compliance assessment prior to implementation. AI systems that pose an unacceptable risk or that constitute a threat to EU fundamental rights have been prohibited, with some exceptions. As explained in Annex III to the AI Act, using AI in the financial market will typically involve high-risk systems, giving rise to certain obligations for financial institutions. They will have to register these systems in a special EU register, making them subject to relevant testing, compliance assessments and audits. AI decisions must also be subject to human oversight (the ‘human-in-the-loop’ rule). Proper management of risks and the quality of data is also necessary to limit discrimination and bias among users of financial services.

Table 1. Summary of AI Act compliance requirements (for high-risk systems).

Requirement	Description	AI Act reference
Risk classification	Must determine if the system falls into unacceptable, high-risk, etc.	Arts. 6–9, Annex III
Conformity assessment	Technical and documentation checks for high-risk AI	Arts. 19–24

Human oversight	Human-in-the-loop must monitor, override or validate AI decisions	Art. 14
Data governance	Training data must be relevant, representative, free of bias	Art. 10
Transparency obligations	Users must be informed of AI use, especially if interacting with it	Art. 50
Post-market monitoring	AI providers must track performance, report issues	Art. 72

While the AI Act acknowledges the importance of the financial market as an integral part of the EU's internal market, as outlined in Article 26 of the Treaty on the Functioning of the European Union (European Union, 2012), it should be considered supplementary to the current EU financial market regulations. This is particularly relevant for market segments that use AI. Financial institutions will be required to fulfil obligations arising from the use of AI in their activities, while also complying with sector-specific requirements. While this will arguably give rise to extra costs, the overriding objective is to ensure safety and trust among clients using specific solutions. This also implies that AI will not impact the lives of those not using the services; in other words, it will not affect those who do not need to use them, nor will it prevent them from exercising their right to opt out of digital technology. While the latter is certainly possible, the significance of these services in daily life may well coerce consumers into using digital technology. Examples of EU legislation where the paths of AI and the financial market converge include the following acts, which cover the FinTech sector:

- Digital Operational Resilience Act (DORA) (European Parliament and European Council, 2022) on cybersecurity and the operational resilience of financial institutions (Zalcewicz, 2023),
- Payment Services Directive (PSD2), standardising electronic payments, security and open banking (Dybiński, 2025, pp. xiii–xiv),
- Markets in Crypto-Assets Regulation (MiCA) (European Parliament and European Council, May 2023) a regulation of the crypto-asset market (Fedorowicz, 2021a; Mariański, 2024),
- Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) (European Parliament and European Council, May 2024), a system of regulations and obligations designed to prevent money laundering and terrorist financing,
- selected European Banking Authority (EBA) guidelines, formulating requirements concerning, for example, risk management, transparency and use of data. Examples of these include the EBA guidelines on loan origination and monitoring (EBA, 2020), on internal governance (EBA, 2021), and on ICT and security risk management (EBA, 2025).

One cannot ignore two other important EU initiatives currently being worked on by European Union institutions, which are the:

- Financial Data Access Regulation (FIDA) (European Parliament and European Council, 2023c), intended, among other things, to enforce transparency on algorithms that use financial data,
- Payment Services Regulation (PSR) (European Parliament and European Council, 2023b), intended, together with the subsequent third generation of PSD2 commonly referred to as PSD3, to form a tandem to improve payment security, promote open access to financial services and strengthen consumer protection.

The above regulations confirm the thesis of a rapidly growing EU financial market that will undoubtedly continue to play an increasingly important role in everyday life. Furthermore, the scope will certainly encompass FinTech institutions offering AI-based instruments. Currently, it is difficult to evaluate the effectiveness of the measures implemented to safeguard individuals' interests, and further research in this area is required.

Such studies should also consider the autonomy of AI-powered systems and the impact of AI-driven decisions on consumers of financial services. This brings us back to the question raised at the beginning of the article: Who is actually responsible for this decision? Will it be humans or code, as described by Lawrence Lessig? His theory of the four modalities is highly relevant to deliberations on the scope of AI application in the financial market, particularly with regard to consumers' right to opt out of digital technology. In reality, however, consumers are in a state of digital compulsion as a result of these modalities. Lessig's theory identifies the following four modalities (or models) that regulate human behaviour:

- Law: the formal rules backed by state coercion (laws, regulations, fines, penalties),
- Norms: social norms that are culturally acceptable or expected,
- Market: identified with economic forces: pricing, incentives, competition,
- Code (Architecture): the physical or logical structure of the environment (especially software code).

As Lessig (1999, pp. 87–89) explains, each of these modalities constrains behaviour in different ways. They are not merely models of law creation in the traditional legislative sense; rather, they are four regulatory forces that shape human behaviour. This is especially relevant in the digital environment (Dolniak et al., 2024); they interact and complement each other. This is evident in financial market regulation, where traditional legal rules must consider market realities and societal habits and customs. There is also room for a fourth modality: code which seems to be the centre of attention, embedded in Lessig's statement that:

Code is law. This code poses the greatest threat to, and offers the greatest promise for, liberal and libertarian ideals. We can design cyberspace to protect values that we believe are fundamental, or we can design cyberspace to allow those values to disappear. There is no middle ground. Every choice involves some kind of construction. Code is never found; it is only ever created, and only ever created by us. (Lessig, 1999, p. 6)

As has already been demonstrated, code certainly shapes the space in which we function, influencing, if not outright creating, our choices through the use of specific techniques. One example is Thaler's and Sunstein's concept of 'nudging', which uses elements of behavioural psychology and choice architecture to encourage people to make decisions in a certain way (e.g. through advertising), without constraining them (Thaler & Sunstein, 2009, pp. 134–146). This raises questions about how this code is used and the limits of its autonomy and control. Although it is admittedly designed by humans, might its design, perhaps reinforced by its self-development, result in it becoming a self-enforcing law and a new incarnation of the legislator-regulator? The effectiveness with which the aforementioned EU legislation is implemented and enforced is crucial. Naturally, this will require highly specialised knowledge to understand and accept the solutions before they are applied, and to supervise their subsequent use (Fedorowicz & Zalcewicz, 2024). At the same time, we must be aware of Decentralised Finance (DeFi), a system of financial services based on blockchain technology that operates without traditional intermediaries such as banks, stock exchanges and supervisory institutions (Bilski, 2024). DeFi relies on smart contracts, sets of self-executing rules based on blockchain technology. As social norms evolve in response to modern technological advances, the openness, automation, decentralisation, immediacy and interoperability of the DeFi system are likely to strengthen its position as a key element of the global financial market (Roukny, 2022, pp. 14–16).

Looking ahead, one might conclude that regardless of the extent of control over the financial market, the most powerful tool for controlling our reality will be the rules governing it, whether created by the EU or by DeFi code. In combination with AI, these rules will effectively eliminate the possibility of opting out of digital technology. This will be the case even if the law does not formally impose an obligation to use these technologies. Individuals will be faced with the choice of either 'taking advantage' of technological coercion or facing financial exclusion. This will be facilitated by Lessig's four modalities combined: law (which encourages technological development), the market (which offers no alternative), social norms (which enforce compliance with the majority's rules) and code (which links all the modalities and is the key tool in creating our contemporary brave new world).

Conclusions

Looking to the future, it is clear that the 21st century will be remembered as a pivotal era in human history. This will largely be due to the technological revolution and the creation of AI. AI would not have been possible without the power of the human mind, whose creativity and abilities will lead to further inventions, which, if used wisely, should facilitate further progress. Hopefully, this will also be the case with AI, a tool with enormous potential that nevertheless raises many questions about its future evolution. Just as humans were present at the birth of AI, they should assist in its development, providing guidance and imposing limitations where necessary. After all, humans are curious beings who ask questions about life and the times in which they live; they are both aware and doubtful. AI, on the other hand, is merely a tool – albeit a powerful one – lacking inner awareness and the ability to reflect on existential questions.

Therefore discussions on the development of AI should emphasise the importance of human involvement in shaping the relationship between technology and traditional values, as outlined by Huxley with his *Savage Reservation*. It is these relationships that have enabled humanity to develop technology and reach the present day. Is the right to live offline as real as the right to freedom of speech? Or has it become more of a fiction? Do we still have the right not to use digital technologies, and is this right protected by law and other regulatory measures? Or has it already become an anachronism in the digital dogma of modernity? The answers to the last two questions are not optimistic for those who see freedom from digitalisation as a fundamental human right (Jóźwicki & Szoszkiewicz, 2025). The analysis conducted in this study concludes that while certain guarantees remain in place in theory, they are gradually being marginalised in practice, and in some areas are becoming illusory. The possibility of opting out of digitisation processes is increasingly purely declarative, and economic, regulatory and social pressures mean that the right to digital opt-out ceases to function in reality. After all, it seems that financial markets and the regulations that govern them enforce the use of digital tools. Rather than neutralising digital compulsion, many EU regulations actually strengthen it.

However, this does not mean that we should stop debating the need for technical alternatives that would allow consumers to retain the option of non-algorithmic decision-making on important matters in their lives (i.e. decisions made by a human being, not a code). We should also consider introducing a right to digital opt-out and including an impact assessment mechanism in the lawmaking process to analyse the use of digital technologies. To many reading these words, this proposal probably seems like science fiction. Perhaps. However, we must also remember that the law should be fair; at its core, it should be based on an axiological system. Although this view may be considered revolutionary in modern times, we should remember that the purpose of law is to protect and develop humanity, not to destroy or subjugate it.

REFERENCES

- Armour, J. (2016). The financial system. In J. Armour, D. Awrey, P. Davies, L. Enriques, H. J. Gordon, C. Mayer, & J. Payne (Eds.), *Principles of financial regulation* (pp. 22–50). Oxford University Press.
- Bauman, Z. (2006). *Płynna nowoczesność*. Wydawnictwo Literackie.
- Bilski, A. (2024). Blockchain i smart contracts w sektorze bankowym. In K. Szpyt (Ed.), *FinTech. Nowe technologie w sektorze bankowym* (pp. 35–52). C.H. Beck.
- Boden, A. M. (2020). *Sztuczna Inteligencja*. Wydawnictwo Uniwersytetu Łódzkiego.
- Bybee, J. K. (2016). *How civility works*. Stanford University Press.
- Chłopecki, A. (2018). *Sztuczna inteligencja – szkice prawnicze i futurologiczne*. C.H. Beck.
- Cyman, D. (2023). Public interest as a determinant of state influence on the financial market in the European Union. *Studia Iuridica*, 98, pp. 55–56.
- Dolniak, P. (2024). Sztuczna inteligencja w wymiarze sprawiedliwości. In P. Dolniak, T. Kuźma, A. Ludwiński, & K. Wasik (Eds.), *AI na styku prawa i cyfryzacji* (pp. 79–107). Wolters Kluwer.
- Dybiński, J. (2025). Wstęp. In J. Dybiński (Ed.), *Prawo rynku finansowego. Prawo usług płatniczych. Komentarz* Vol. XB. (pp. xiii–xiv). C.H. Beck.
- European Banking Authority. (2020). *EBA guidelines on loan origination and monitoring*, EBA/GL/2020/06. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/Translations/886690/Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring_COR_PL.pdf
- European Banking Authority. (2021). *EBA guidelines on internal governance*, EBA/GL/2021/05.
- European Banking Authority. (2025). *EBA guidelines on ICT and security risk management*, EBA/GL/2019/04. (Originally published 2019).
- Engelen, E. (2008). The case for financialization. *Competition & Change*, 12(2), pp. 111–119.
- European Commission. (2024, 10 June). *Targeted consultation on artificial intelligence in the financial sector*. https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-artificial-intelligence-financial-sector_en
- European Commission, *Overview of digital finance*. https://finance.ec.europa.eu/digital-finance/overview-digital-finance_en
- European Parliament and European Council. (2015, 25 November). Directive (EU) 2015/2366 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and Repealing Directive 2007/64/EC (Text with EEA Relevance) (PSD 2) (O. J. L 337, 23.12.2015).
- European Parliament and European Council. (2016, 27 April). Regulation (EU) 2016/679 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) (Text with EEA Relevance) (O. J. L 119, 04.05.2016).
- European Parliament and European Council. (2022, 14 December). Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) no.

- 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014 (EU), no. 909/2014 and (EU) 2016/1011 (DORA) (Text with EEA Relevance), PE/41/2022/INIT (O. J. L 333, 27.12.2022).
- European Parliament and European Council. (2023a). *Proposal for a Directive of the European Parliament and of the Council on Payment Services and Electronic Money Services in the Internal Market Amending Directive 98/26/EC and Repealing Directives 2015/2366/EU and 2009/110/EC*, COM/2023/366 final (PSD 3).
- European Parliament and European Council. (2023b). *Proposal for a Regulation of the European Parliament and of the Council on Payment Services in the Internal Market and Amending Regulation (EU) no. 1093/2010*, COM/2023/367 (PSR).
- European Parliament and European Council. (2023c). *Proposal for a Regulation of the European Parliament and of the Council on a Framework for Financial Data Access and Amending Regulations (EU) no. 1093/2010, (EU) no. 1094/2010, (EU) no. 1095/2010 and (EU) 2022/2554 (FIDA)*, COM/2023/360 final.
- European Parliament and European Council. (2023, 31 May). Regulation (EU) 2023/1114 on Markets in Crypto-Assets, and Amending Regulations (EU) no. 1093/2010 and (EU) no. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA Relevance) (MiCA) PE/54/2022/REV/1 (O. J. L 150, 09.06.2023).
- European Parliament and European Council. (2024, 31 May). Regulation (EU) 2024/1624 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (AML/CFT) (Text with EEA Relevance), PE/36/2024/REV/1 (O. J. L 2024/1624).
- European Parliament and European Council. (2024, 13 June). Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) no. 300/2008, (EU) no. 167/2013, (EU) no. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance), PE/24/2024/REV/1 (O. J. L 2024/1689).
- European Union. (2012). *Consolidated version of the treaty on the functioning of the European Union* (O. J. C 326, 26.10.2012).
- Fedorowicz, M. (2021a). Nadzór nad rynkiem kryptoaktywów w świetle projektu rozporządzenia MiCA – najnowsze wyzwania i tendencje regulacyjne cyfrowej stabilności i odpowiedzialności na rynku finansowym UE. In K. Królik-Kołtunik & I. Skibińska-Fabrowska (Eds.), *Inwestycje alternatywne – nowe spojrzenie*, (pp. 75–88). CeDeWu.
- Fedorowicz, M. (2021b). Znaczenie soft law EBA dla określania normatywnego standardu ochrony konsumenta na rynku finansowym. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, 10, Article 7, pp. 21–34.
- Fedorowicz, M., & Zalcewicz, A. (2024). Challenges posed to the EU financial market by the implementation of the concept of sustainable financing. *Białystok Legal Studies*, 29, pp. 54–56.
- Footer, R. M. (2020). The EU's engagement with business on human rights. In J. Wouters, M. Nowak, A. L. Chané, & N. Hachez (Eds.), *The European Union and human rights: Law and policy* (pp. 312–344). Oxford University Press.
- Gromski, W. (2007). Law and economics jako teoria polityki prawa. In J. Stelmach & M. Soniewicka (Eds.), *Analiza ekonomiczna w zastosowaniach prawniczych* (p. 51). Wolters Kluwer Polska.
- Huxley, A. (1946). *Brave new world*. Harper Crest.

- Jędrzejczak, M. (2024). Protection of personal data processed in artificial intelligence systems. *Gdańskie Studia Prawnicze*, 64, Article 3, pp. 88–89.
- Jóźwicki, W. W., & Szoszkiewicz, Ł. (2025). Non-use of the internet as human rights enabler? The curious cases of the right to privacy and the right to health. In D. Kloza, E. Kuźlewska, E. Lievens, & V. Veerdoodt (Eds.), *The right not to use the internet: Concept, contexts, consequences* (pp. 106–120). RoutledgePoczątek formularza.
- Jurkowska-Zeidler, A. (2008). *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*. Wolters Kluwer Polska.
- Jurkowska-Zeidler, A. (2011). Nowa globalna architektura finansowa. *Gdańskie Studia Prawnicze*, 25, pp. 535–547.
- Kloza, D., Kuźlewska, E., Lievens, E., & Veerdoodt, V. (Eds.). (2025.) *The right not to use the internet: Concept, contexts, consequences*. RoutledgePoczątek formularza.
- Kowalewska, E., & Musiał, M. (2025). Accessibility of mobile banking apps in Poland: A legal analysis of recent developments. *Przegląd Ustawodawstwa Gospodarczego*, 3, pp. 27–35.
- Krizhevsky, A., Sutskever, I., & Hinton, E. G. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, 60(6), pp. 84–90.
- Kusak, M. (2022). Quality of data sets that feed AI and big data applications for law enforcement. *ERA Forum*, 23, pp. 209–219.
- Kuźlewska, E. (2025). *Non-use of digital technologies and regulation*. <https://bsp.uwb.edu.pl/libraryFiles/downloadPublic/8>
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
- Mariański, M. (2024). Reflections on the possible application of Rome I Regulation to obligations related to crypto-assets. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, pp. 24–28.
- Masłowski, M. (2024). *Otwarta bankowość*. C.H. Beck.
- Nieborak, T. (2016). *Creation and enforcement of financial market law in the light of the economisation of law*. Wydawnictwo Naukowe UAM.
- Nowakowski, M. (2020). *Fintech: Technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*. Wolters Kluwer.
- Nowakowski, M. (2023). *Sztuczna Inteligencja: Praktyczny przewodnik dla sektora innowacji finansowych*. Wolters Kluwer.
- Roukny, T. (2022). *Decentralized finance: Information frictions and public policies. Approaching the regulation and supervision of decentralized finance*. Publications Office of the European Union.
- Rutkowska-Tomaszewska, E. (2020). Prawo ochrony konsumenta usług finansowych w świetle założenia racjonalnego ustawodawcy – kilka wybranych uwag. *Przegląd Prawa i Administracji*, 120, pp. 481–498.
- Rutkowska-Tomaszewska, E., & Gałązka, P. (2024). The role of European supervisory authorities in consumer protection standard setting on the financial services market: Based on the example of the European Banking Authority. *Studies in European Affairs*, 28(2), pp. 223–232.

- Smolak, M. (2001). Jak prawo łączy się ze światem? Uwagi na marginesie książki W. Gromskiego, Autonomia i instrumentalny charakter prawa. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 3, pp. 191–198.
- Stacewicz, P. (2023). O światopoglądowym oddziaływaniu informatyki w świecie współczesnym. In A. Zalcewicz & R. Kędziora (Eds.), *Nowe technologie. Wartości, prawa, zasady* (pp. 305–314). Politechnika Warszawska.
- Szozzkiewicz, Ł. (2021). *Dostępność danych w czasach sztucznej inteligencji a prawa człowieka w dziedzinie nauki*. Wydawnictwo INP PAN.
- Szozzkiewicz, Ł., & Świergiel, R. (2018). Financial institutions and the protection of individuals' autonomy: A human rights perspective. *Roczniki Nauk Prawnych*, 28(4), pp. 125–136.
- Szpringer, W., & Szpringer, M. (2014). Nowe zjawiska w regulacji rynku usług płatniczych (wybrane problemy na tle projektu noweli do dyrektywy PSD). *'e-mentor'*, 56(4), pp. 73–83.
- Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth and happiness*. Penguin Books.
- United Nations. (1948). *Universal declaration of human rights*. <https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf>
- Zalcewicz, A. (2016). Teoretycznoprawne wprowadzenie w problematykę rynku usług płatniczych – kilka uwag tytułem wstępu. In A. Zalcewicz & B. Bajor (Eds.), *Ustawa o usługach płatniczych. Komentarz* (pp. 19–28). Wolters Kluwer.
- Zalcewicz, A. (2023). New technologies in the control of public finances and building public confidence in the state. *Bialystok Legal Studies*, 28(2), pp. 23–25.
- Ziętek, A. (2013). *Jean Baudrillard wobec współczesności: polityka, media, społeczeństwo*. Universitas.