Sulkhan-Saba Orbeliani University

# Contractual Regulation and Legal Protection of Big Data in Digital Financial Market Competition

Thesis submitted for the degree of Doctor of Philosophy

Author: Sandro-Giorgi SARUKHANISHVILI
Supervisors: Associate Professor Nato GUGAVA
Associate Professor Salome KAVTARADZE
Associate professor doc. JUDr. Michal PETR, Ph.D.

Tbilisi, 0186, Georgia,
August, 2025

## Table of Contents

## Abstract

The doctoral dissertation concerns Big Data in the context of the digital economy, examining its economic value, legal regulation, and integration into platform business models. The dissertation analyses the complex ecosystem of Big Data and the related data architecture. Technological progress significantly influences both societal and economic processes, manifesting in the emergence of digital markets and the formation of digital business models. In this process, Big Data play a crucial role, characterised by the collection of large volumes of heterogeneous, often unstructured information from numerous digital sources at high speeds.

The effective use of Big Data requires a comprehensive Big Data ecosystem and corresponding architecture that facilitates the collection, storage, processing, and generation of value from data. The Big Data ecosystem, in turn, represents a specific form of the digital ecosystem, integrating data owners, analytics companies, professionals, cloud service providers, as well as the academic and business sectors. Data architecture defines the types, models, and structures of data, serving as a fundamental component of the ecosystem. Its purpose is to manage the data lifecycle, ensure integration, and guarantee data quality and security.

A complex Big Data ecosystem transforms data into economic value, turn Big Data as an economic resource and intangible property with both economic and legal significance. Data buying, selling, transferring, and processing are increasingly conducted for direct commercial purposes. The effective use of data is impossible without platforms that connect data producers and consumers.

The objective of the research is to explore the role of digital platforms as "gateways" in the collection and processing of Big Data within digital financial markets and to study legal mechanisms that protect Big Data as a form of property. The thesis covers the analysis of Big Data and digital markets, discusses the peculiarities of competition in digital markets, evaluates the role of platforms in contractual relationships, identifies legal challenges, and formulates recommendations.

Specifically, there is a need to develop legal approaches that establish standards for protecting structured Big Data in platform-based contractual relationships, promote fair competition in digital financial markets, and safeguard the rights of both individuals and legal entities. The research focuses particularly on the development of fintech companies in the financial sector, and the roles of artificial intelligence and distributed ledger technologies in financial services.

The importance of Big Data in the financial sector, especially with the growth of fintech companies, is becoming even more pronounced. The development of data ecosystems and architecture based on platforms enables the sourcing, storing, and processing of data collected from various origins within a single space. This process emphasizes the significance of cloud services and the legal protection of data through mechanisms such as commercial secrets, personal data protection, and intellectual property regimes.

Access to Big Data is gradually becoming a decisive factor in achieving dominance in digital markets. Companies with exclusive access to data can establish dominant positions, leading to market concentration and restricting innovative development. Fintech companies collect both personal and non-personal data from various sources, such as online services, registration forms, and user behaviour analysis. Banks, as the core of the financial system, are particularly active in this sphere, creating "private knowledge networks" that grant them a competitive advantage.

Therefore, regulating access to data and limiting platform power has become a central issue for both national and international legal frameworks. The dissertation also addresses the legal aspects of digital contracts and smart contracts, as well as the role of distributed ledger technologies in ensuring Big Data security. It provides a legal analysis of the digital market, the protection of Big Data, and the need to develop a normative environment capable of responding adequately to technological challenges.

Particular emphasis is placed on data security, legal regulation, platform economy governance models, and the legal status of Big Data as an economic asset. Accordingly, the thesis discusses the current state of Georgian legislation, compares it to European Union regulations and directives, and identifies gaps within Georgian law. It stresses the necessity of defining the legal status of platform services.

Based on EU experience, the thesis underscores the importance of regulating digital markets by controlling the activities of "gatekeepers," thus ensuring fair competition, protecting consumer rights, and encouraging innovation. The widespread practice of data collection by platforms under standard contractual terms requires a stricter legal framework to prevent market abuse.

The issues of competition regulation in digital markets, the importance of data access, and the differentiation of data markets are central themes of the dissertation. It offers definitions for the Big Data market and the relevant market for Big Data. The complex Big Data ecosystem, as a value-creation mechanism, involving the collection, storage, processing, and business-use of data, constitutes a data market, while its various layers represent the relevant market for Big Data.

It is notable that current EU regulations, such as the GDPR and PSD2, aim to protect data and ensure competition in digital markets. However, in practice, large tech companies with substantial resources often benefit the most from these regulations by adapting more easily. In this context, Georgian legislation requires expansion and modernisation — for instance, the establishment of a "gatekeeper" status and the setting of new standards for data collection and usage.

The dissertation demonstrates that Big Data, as an intangible property, requires special legal protection to ensure that businesses and individuals feel secure in digital markets. Therefore, it is advisable to develop additional regulations in Georgian law, such as a dedicated law on trade secrets and a more detailed definition of platform services within the framework of the "Law on Electronic Commerce." The research highlights the necessity for legal policies to keep pace with technological advancements to safeguard human rights, ensure fair competition, and foster an innovative, secure, and transparent digital economy.

# I. Introduction

With the advancement of cutting-edge technology, society is becoming more complex, and human actions are increasingly digitised. The digital world has become an inseparable part of human life – digital technologies, social media, and other technological innovations are embedded in our daily routines. A "digital revolution" is underway – the digitisation of information – which has enabled the processing, storage, and transmission of vast amounts of data in real time. The spread of internet-connected products has increased the volume and potential value of data for consumers, businesses, and society.

The growth of modern technologies has fostered the development of digital markets, which are integral to the digital economy. In digital markets, firms operate as platforms through which various products are sold to different groups. The models of large technology companies (Big Tech) are platform-based, and their typical activity includes a wide range of general digital services such as search engines, social media, e-commerce, telecommunications, etc., with data being their primary currency. To provide digital services, companies usually build platforms through which transactions occur between businesses and consumers.

Digital innovations are also transforming financial services. As a result, large technology companies are expanding into economic sectors such as credit, insurance, and financial market funds to meet consumer needs. They act as intermediaries between users and providers of financial products or directly provide loans and investment services — made possible through automated analytics supported by access to massive data resources. The involvement of Big Tech in financial services implies the use of relatively new technologies and tools that are products of recent developments. These include artificial intelligence, big data, cloud-computing services, and distributed ledger technologies (DLT).

Accordingly, digital services have been created that unite the world and form a single, global market. Through the platforms developed by companies for delivering digital services, transactions occur between businesses and consumers. These platforms act as "gateways" that have significant influence in the digital market. "Gatekeepers" control one or more gateways and maintain or will maintain entrenched and durable market positions. As a result, businesses become increasingly dependent on the acquisition and processing of big data. The misuse of personal data is rising, even though personal data held by companies has economic value. This creates a need for protection and the development of approaches that better safeguard human rights.

Big data refers to increasingly large volumes of information, closely tied to personal data. Its processing brings legal consequences, to which legal systems are not immune. In fact, digital

transformation has altered legal structures, with artificial intelligence — based on algorithms — taking over many functions. With the advancement of technology, the use of large volumes of personal data also grows. In turn, digital innovations affect industrial organizations, including traditional financial industries — for example, big data could replace material collateral. Big data influences human social behaviour and the formation of will, as decisions are often based on feelings and emotions, and big data can influence those decisions.

In a rule-of-law state, individual rights are of paramount value. Human rights form the foundation of values without which life would be unliveable and inappropriate. The function of a legal state is to protect the rights of individuals and members of society. In the context of human rights protection, personal data protection is essential. When legislation does not keep pace with technological development, the legislature must regulate newly emerging relationships, as law and legal policy are closely intertwined.

In this regard, the European Union declares that artificial intelligence must serve human welfare, and everyone should benefit from the advantages of intelligent systems and algorithms without violating fundamental rights.

The protection of personal data in Europe began in the 1970s when several countries adopted legislation to control the processing of personal information by public authorities and large corporations. Later, data protection instruments were developed at the European level. Over time, personal data protection was increasingly regulated by higher-level institutions such as the Court of Justice of the European Union. As a result, personal data fell under a distinct protection regime. Notably, EU law views data protection as separate from the right to private life.

The European Union has developed the Digital Markets Act, which is closely connected to the EU Charter of Fundamental Rights, the European Convention on Human Rights and Fundamental Freedoms, and the General Data Protection Regulation (GDPR), emphasizing the importance of these legal instruments for regulating big data within the digital market. Moreover, firms that hold dominant market positions and collect data from users have little incentive to protect that data if there is minimal competition. To ensure a fair digital environment for individuals, businesses, and especially SMEs, the EU aims to create a secure digital space based on competition where fundamental rights are protected, and consumers and clients are safeguarded across a unified digital market.

Accordingly, the role of gateways — especially those held by large players — will be clearly defined. The EU will also ensure transparency, open technologies, compatibility, and standards to foster trust in technology and allow users to make autonomous, informed choices.

The objective of this research is to analyse the legal framework and standards for collecting and processing big data in digital financial markets, particularly in the relationship between "gateways" and users. The aim is to ensure that structured big data, as a proprietary asset, is protected within contractual relationships between data collectors and platforms and that dominant market players in digital financial markets are prevented from abusing their position.

The study seeks to address the legal issues involved in trade transactions by protecting both the proprietary rights of individuals — enabling them to benefit from structured big data — and the personal data of both natural and legal persons. The work aims to explore ways to promote fair competition through the protection of large-scale personal data and evaluate the role of the state in ensuring legal protection of big data under competitive conditions. The goal is to regulate the use of big data in contractual relationships between parties and ensure that individuals can protect their rights through legal principles and judicial remedies.

The thesis is structured into seven parts. Parts I and VII serve, respectively, as the Introduction and the Conclusion. The core research is presented in Parts III–VI. Part II is dedicated to an overview of the research method and methodology. In Part III, the challenges of big data and the digital market are outlined; Part IV examines the nature of competition in digital markets and the influence of big data; Part V analyses the standard contractual terms that platforms offer users in digital transactions and investigates the rights platforms possess when processing big data; and Part VI puts forward a series of recommendations.

## Chapter II.
## Research Method and Methodology

New technologies and an ever-changing environment are reshaping the boundaries and frameworks within which law is created, interpreted, and subsumed. Consequently, existing legal concepts and approaches must be adapted to address these technological developments. Legal methods, in turn, are not merely tools for locating the appropriate provision in a code to apply rules to facts. It is important to note that legal reasoning often extends beyond the written text and incorporates external sources such as legal history, expert testimony, precedents, and scholarly writings. These elements contribute to providing the necessary context for interpreting and applying the law. Moreover, the rapid pace of technological advancement necessitates the development of principle-based regulations, as technology frequently evolves faster than the legal system can respond.

Interpretation is one of the essential features of law, and it is carried out differently by judges and legal scholars. Primarily, interpretation involves determining the meaning of the language of the written text. Secondarily, it entails interpreting that text as a legal object – such as a contract or a code – in order to establish its legal content, specifically the legal consequences that will follow from adopting or implementing a particular interpretation of the law. Arriving at a correct legal answer may also involve the use of analogies and an understanding of general principles.

For Ronald Dworkin, interpretation engages in profound debates around key concepts such as dignity, justice, and liberty. Interpretation, in this view, requires normative reasoning in the process of resolving legal conflicts. While the law is, of course, a human construct, legal interpretation plays a crucial role in clarifying the meaning of written norms to achieve their intended purpose.

Furthermore, legal philosophy has the capacity to enrich legal doctrine and support the development of the discipline. Thus, combining descriptive analysis with normative analysis is essential for understanding law as a coherent and unified concept. Accordingly, in the context of legal interpretation, philosophical and dogmatic perspectives of law will play a vital role – especially in rapidly evolving technological environments –by enabling a systematic approach to determine the legal mechanisms available for the protection of big data.

It should be noted that algorithmization requires thinking through a variety of socio-cultural categories such as subjects, actions, responsibilities, and knowledge. Academic legal scholars can explore various methodologies by collaborating with experts from other scientific disciplines and incorporating interdisciplinary findings into their research. Accordingly, understanding the market is crucial for grasping the value of big data, the legal frameworks that govern it, and the corresponding legal protection mechanisms.

The market itself is an institution and a central object of economic study. Economic theories influence the structure and operation of markets, particularly given the close interconnection between competition law and economics. Economists examine how markets function, with a primary focus on facilitating the exchange of goods and services and reducing transaction costs associated with such exchanges. Modern markets often no longer require a physical space for transactions, as these increasingly occur via online platforms. As a result, buying and selling in such markets necessitates corresponding legal rules to ensure the protection of rights and responsibilities involved in platform-based transactions.

Importantly, when examining how law influences the economy, economic analysis of law does not treat law as an independent variable. Rather, it views law as an integral part of the legal system – a source of authority and behavior that directly affects economic outcomes. This

type of analysis emphasizes the role of risks and sanctions in shaping compliance with the law. However, values such as legitimacy are equally – if not more – important in fostering legal obedience. Therefore, **the interdisciplinary character of methodology is essential in the study of the topic addressed in this dissertation**, as it allows for a more comprehensive and context-sensitive analysis of the intersection between law, technology, and economic structures.

Within the scope of this research, a comparative legal method is employed to examine the legislation of Georgia, the European Union, and selected EU Member States in relation to data protection, trade secrets, and copyright. The analysis also includes decisions of the Georgian courts as well as the jurisprudence of the European Court of Justice, as the institution responsible for interpreting EU law. Additionally, publicly requested information from the Georgian National Competition and Consumer Protection Agency and the National Bank of Georgia has been analysed, particularly regarding the implementation of necessary measures and the existence of regulations pertaining to the oversight and regulation of big data and the platform economy. The study further explores the interplay between big data and competition in the digital market, with the aim of identifying gaps in the legal framework that, on the one hand, support the protection of personal data, and on the other, promote the principle of fair competition.

## Chapter III
## The Legal Status of Big Data in the Digital Economy and Its Relation to Intangible Property Rights

Chapter III explores the multifaceted legal and economic dimensions of big data within the competitive digital financial market. It offers a comprehensive exploration of the **relationship between big data and the digital economy**, emphasising both the technological and legal dimensions of this connection. The chapter opens with a classification of **big data types**, distinguishing between **structured, unstructured, and semi-structured data**, and introducing the concept of **"big personal data"** to highlight the increasing volume of personal information collected in the digital space. It can be said that *big data* refers to a heterogeneous collection of various types of data, facts, or information in digital form, characterised by unlimited operations, which are collected at high speed from multiple sources and processed in real time using advanced technologies. Big data is stored in its raw form, extracted using algorithms developed through machine learning and based on empirical analysis. What distinguishes big data from ordinary data is its high speed, variety, and volume. Its sources are numerous, but

social media, machine-generated, and transactional data are the three main ones. Moreover, data processing produces new data, which itself can become big data. According to types, big data can be structured, semi-structured, or unstructured. However, regardless of the type, processing big data requires powerful software, algorithms, next-generation technologies, and architecture.

The discussion then shifts to the **digital economy and modern business models**, focusing on how **information society services** and **platform-based services** function as core components of this new economic environment. It underscores the significance of platforms in data-driven commerce and their growing influence in shaping legal and regulatory frameworks. the terms *platform* and *platform-based service* are defined and highlighted that they are not interchangeable. A platform is a collection of markets, a type of market, where information society services are provided. It is a structural unit of the digital economy that connects market participants – specifically, service providers and consumers – and ensures digital service delivery (via websites or applications). It requires high-tech architecture, algorithms, and network interaction. A platform can be used for various business models. Platform-based services are part of the online services provided by the platform. Unlike information society services, platform-based economy is not recognized by Georgian legislation. However, the criteria for information society services include platform-based services as well. Therefore, platforms – as part of the digital economy and a collection of markets that provide information society services – fall under the regulatory domain of Georgia's National Competition Agency, except in cases where platform markets are regulated by other authorities according to the law.

Next, the chapter delves into **data acquisition and processing**, describing the **Big Data Complex Ecosystem and Big Data Architecture** and detailing the types of data collected by **digital market agents** – including **machine-generated data** and information from the **Internet of Things (IoT)**. It also explores the **structuring of data**, the role of profiling, and the **oversight mechanisms** implemented by digital platforms. A data ecosystem is an information-technology infrastructure – a combination of different systems for collecting, storing, and using data from various sources. In contrast, *data architecture* is a part of the data ecosystem that defines how data should be processed, stored, integrated, and used within an organisation for its production goals. With the help of a big data complex ecosystem, this data is collected, transmitted, and converted into monetary value. Big data has economic value for companies and, therefore, practical utility. In economics, big data is used to drive innovation and to deliver targeted, updated, and improved products and services. Practical application of big data requires the establishment of a big data ecosystem. In turn, companies develop big data architectures to

support this ecosystem in achieving their business objectives. Big data architecture helps companies reduce costs and make timely, well-informed decisions. Thus, both material, financial, and intellectual resources are invested in the creation and processing of big data to derive results. It is noteworthy that Georgian legislation partially addresses the Big Data Complex Ecosystem and Big Data architecture, particularly in the context of platform, software, and infrastructure services. Specifically, this applies to the cloud service model, which involves providing users with data storage, networking, computing, and processing resources, all embedded within the infrastructure of the cloud service provider. Accordingly, Georgian law recognizes the big data complex ecosystem and data architecture in terms of cloud services, but regulation applies only when the big data complex ecosystem and architecture themselves constitute the service or product.

The chapter begins by examining the role of fintech companies, focusing on how they operate under conditions of big data-driven competition and integrate into the evolving business models of the financial sector. The platform-based economy holds a significant position in the digital economy. It serves as a collection of markets, a business asset, and a tool for conducting digital economic activity electronically. For businesses to develop and operate business models typical of the digital economy, integration of technological architecture and digital engineering is necessary. Consequently, financial institutions in the digital marketplace create *FinTechs* which eliminate the need for intermediaries in business relations, disrupt existing industrial structures, and have the ability to utilize large databases sourced from multiple, unrelated origins. Therefore, financial institutions purchase cloud services and create platforms, which, on the one hand, become part of the big data complex ecosystem, and on the other hand, part of information society services. It must be noted that *Information society services* is a broad term that includes platform-based services, as well as any electronic, fee-based service – including cloud services provided by financial organizations. Therefore, FinTech fit into the criteria of information society services in two ways: first, as a big data complex ecosystem, and second, as a method of providing intermediary services through electronic means. FinTech, as part of the big data complex ecosystem, collect data from users and transmit it to the data architecture for processing. After processing and contextualizing the data, the knowledge gained is used by businesses to maximize profits. Georgian legislation only addresses risk issues related to financial institutions adopting cloud service models or platform-based services. It does not regulate measures for protecting large-scale data.

The second part of the chapter focuses on **big data as an intangible asset**, examining its intersection with **intangible property rights**. It analyses how big data acquires **economic value**, the **practical needs** that drive its commodification, and how this translates into potential

**property rights**. The chapter concludes by discussing the **legal regulation of big data's property value**, laying the groundwork for recognizing data as a legally protectable economic good within the digital economy. Big data can be bought and sold, transferred to third parties either as ready-made records or as data collected and processed via the Internet of Things (IoT), granting it not only economic but also property value. It can be said that the concept of *property* includes anything that can be expressed in material value, has sufficient characteristics for civil circulation, has economic value, brings financial benefit to a physical or legal person, serves as a source of property rights, and can be owned, disposed of, and used. Therefore, it can be protected from infringement so that its lawful owner can gain material benefit or claim his/her rights against another person. Therefore, big data is an *intangible property asset*. It holds both economic and property value and can be bought, sold, owned, disposed of, used, and protected from infringement so that its lawful owner can gain material benefit or claim rights against another person.

Finally, it discussing the need for regulatory frameworks that recognise its property value. It worth to mention that none of the existing legal regimes related to data protect big data specifically. Some regimes protect collections of structured data, while others provide limited protection for data ownership – without referring to it as a "property right." In Georgia, copyright and trade secret protection regimes fail to offer even the minimum level of protection for big data that is possible under the European Union framework. According to Georgian legislation, the proprietary rights of a database creator or the holder of copyright over it are protected only if the database qualifies as a "work" – that is, the result of intellectual and creative activity – or if a significant investment was made to improve it. Furthermore, such databases must be systematised. In light of this, structured big data can only be considered a subject of protection if resources have been invested in it, including both human and financial resources. Conversely, data collections created by machines cannot be protected, and unstructured or semi-structured data cannot be protected at all. Additionally, some parts of the information contained within these databases may not be legally protected, even if the information is significant or valuable. To protect valuable or important information, it may be possible to apply the concept of a trade secret. However, in such cases, the owner of the trade secret must declare it as such, and the protection of the trade secret must serve to safeguard the owner's normal operations and functionality. Unlike the European Union and the United States, Georgian legislation does not include information with potential economic value under the concept of a trade secret.

Overall, Chapter III bridges the gap between the **technological reality** of big data and the **legal challenges** of its classification, ownership, and regulation in the evolving digital markets and marketplaces.

## Chapter IV
## Contractual Regulation of Big Data

Chapter IV examines the intersection of contract law and the digital market, focusing on the unique challenges and opportunities presented by the rise of digital contracts. It begins by exploring the nature of digital contracts, categorizing them into various types and highlighting their growing significance in modern transactions.

An **electronic or digital contract** is a form of digital content. It originates and is delivered electronically, created as an **electronic document**, and concluded using electronic means, in accordance with general rules for contract formation. The subject of an electronic contract can be **both digital services and products**, as well as any service that implies a contractual obligation between a trader and a consumer. In the formation of an electronic contract, a **third party plays a significant role** – namely, the provider of electronic services. This third party creates services necessary for fulfilling the formal requirements of an electronic contract, such as **electronic signatures, electronic seals, creation of authentication certificates, their storage, and verification**. Furthermore, **Distributed ledger technologies (DLTs)** are used for managing transactions, recording contracts, storing records, verifying contracts, and ensuring data security. These technologies are built on **layered architecture**, where each layer performs a specific function, – each layer in this technology is responsible for a specific task:

- The **protocol layer** defines the rules and coded architecture;
- The **network layer** enforces the protocol;
- The **data layer** defines and clarifies the data used to reach agreement.

DLTs are a **natural foundation for applications such as smart contracts**. A smart contract is a type of electronic contract—**computer code** that digitally encodes the terms of a transaction. These contracts can be concluded between **business operators, individuals, or even machines**, and their execution is **automatic**.

The chapter further investigates the validity of digital contracts, addressing the legal frameworks and requirements necessary for their enforceability. It delves into the relationship between the technological aspects of digital contracts and the law, analysing how advancements in technology influence the legal recognition and regulation of digital agreements. I**nternational and European law provide the basis for the legal validity** of

electronic contracts. For an electronic contract to be legally valid, it must satisfy the **general requirements of contract formation**. This requires analysis of the **function and role of electronic means**, specifying all the relevant details of how the electronic contract was concluded using these technologies. As for smart contracts, to establish their legal validity, one must analyse the **software code** and the **technology** in which the contract is created, concluded, and executed. To determine the **legal nature of smart contracts**, every layer of the distributed ledger technology must be examined – whether the contract complies with legal requirements, whether it violates any legal norms of a given jurisdiction, whether **the parties' intention was clearly expressed**, and what conditions make the contract enforceable. The **validity of a smart contract** also depends on its connection to **natural (spoken) language**. A smart contract will be considered legally binding if the **parties' intent and mutual agreement are clearly expressed**, and if the **subject matter** of the contract is **appropriate and reasonable**.

In summary, the transformation of the economic order by **digital economy** requires the regulation of contractual relations in a manner that includes both **legislative frameworks and judicial practice**. A digital contract, being a digital content product, is created as an electronic document using electronic means and must comply with general contract formation rules. **Smart contracts**, a form of electronic contracts, operate through DLTs. They are computer codes concluded between business operators, individuals, or machines and are executed automatically.

The second part of the chapter shifts focus to big data and its impact on digital contracts. It discusses the technological aspects of contractual relationships, examining how big data plays a role in shaping the formation, negotiation, and performance of contracts in the digital landscape. Additionally, the chapter explores the impact of big data on the substance of contracts, considering how the vast amounts of data influence contractual terms, obligations, and execution in the digital economy.

By nature, **DLTs are a component of the big data ecosystem**, designed to comply with legal standards and operate accordingly. However, **data produced and used within DLTs remains outside the scope of legal control**. There is no regulation or oversight over such data, because in a **decentralized architecture**, each participant in the supply chain controls their own data and does not share it. Participants rely on a **trusted third party** for data exchange; in this process, **data becomes a product**, and those who use it become **consumers**. It must be noted that **digital contracts generate and utilize big data** during their formation, execution, and operation—data that is associated with the parties to the contract. However, in some cases, parties to a digital contract **do not have access to the data** generated from their business activities, including data necessary for **statistical calculations**. Accordingly, **only decentralised**

**DLTs can ensure the security of big data** for the parties generating it. If the DLT is centralised, then control over it is possible. However, **laws must introduce additional requirements** for validating contracts that use decentralised DLTs. Specifically, the validity of such contracts should depend on the **legality and licensing** of the services provided by the **trusted third party** involved.

This chapter provides a comprehensive analysis of how digital contracts and big data are reshaping traditional contractual practices in the digital market.

## Chapter V
## Competition in the Digital Financial Market

Chapter V provides a comprehensive analysis of how big data and its associated competitive dynamics influence the digital financial market, offering a nuanced understanding of the interplay between data, competition, and innovation in the financial sector. It worth to mention that competition is crucial for market development, as it is a regulated form of rivalry based on the principle of equal rights for economic agents. For the purposes of competition, innovation is of decisive importance. Restriction of innovation is considered a barrier to competition. Big data, in turn, supports the development of innovative business models, products, and practices by entrepreneurs. It is used for updated strategies and the implementation of innovations. Data is collected and sold on the data market. Recognising the economic value of data by competition authorities has made it possible to apply competition law to companies' behaviour in collecting and processing data.

The chapter delves into the critical relationship between big data and the digital financial market, exploring how data-driven ecosystems are transforming financial markets. It begins by examining the concept of the relevant market in the digital economy, offering insights into how traditional market boundaries are reshaped by digital innovation and big data. Thus, a digital market refers to the market for a specific digital service (a digital platform), for example, a specific platform providing a particular digital service, such as Amazon, Spotify, or Facebook. Accordingly, it can be said that the market of a digital ecosystem is a combination of markets for various types of primary and secondary products, where the primary and secondary products are interdependent and interconnected, either technologically or through technical compatibility. The relevant market is a dynamic concept and its definition is broad. The relevant product market encompasses an area with common conditions for the sale of goods, defined by specific suppliers (sellers) and consumers (buyers), where a commercial relationship

is established between them. Determining the relevant market involves analysing its boundaries – specifically, defining its product boundaries, geographical scope, and time frame. However, under the conditions of the digital economy, the geographical dimension becomes a less appropriate criterion for the purposes of competition law. Therefore, the digital market should be considered separately from the non-digital market. Moreover, in the digital economy, there is no universal method for determining the relevant market that applies equally to all cases. To define the market, one must assess the distinctive elements of the digital economy – particularly, identifying digital infrastructure, e-commerce tools, and electronic intermediaries that connect consumers and suppliers, which may involve both paid and free services. Furthermore, when identifying digital markets, it is necessary to consider the influence of the digital ecosystem, particularly whether there are relevant markets for the primary and secondary products or if the digital market represents a "frame" of a single digital platform. For competition law purposes, it is advisable to consider the nature of the service, and the actual conditions of the market's structure and functioning.

Regulating competition in digital markets is closely tied to gatekeepers that provide core platform services. Core platform services are diverse and include online intermediation services, online search engines, social networks, video-sharing platforms, advertising services, and more. Two- and multi-sided (multi-layered) platforms are characteristic elements of digital markets. In two-sided platforms, buyers and sellers are directly connected, with the platform itself selling a service or product. In multi-sided platforms, a third party enters for selling products or services to the buyer, while the platform provides the space for this interaction. It is important to note that many services offered by platforms do not involve monetisation; however, the non-monetised layer of a market can still be considered part of the platform market (as a relevant market). The revenue-generating side of the market is a good starting point for defining platform markets, but this approach should also be extended to the market's free layers.

The chapter then focuses on the relationship between big data and the digital financial market, highlighting how the collection, management, and exchange of big data are essential components of the modern financial landscape. Further, the chapter explores the structure of the big data market, analysing how data flows within the digital economy and the ways in which various actors interact with it. The chapter also investigates the dynamics of competition for big data markets, including the role of platforms in controlling access to valuable data and the competitive pressures financial platforms face as they vie for data dominance. In particular, it discusses how platforms manage access to data and the competition among financial platforms for access to and control over data markets.

The big data market consists of the interconnected and interdependent chain of production and value creation of big data. As such, the complex ecosystem of big data constitutes the big data market, and its individual components make up the relevant big data markets. Additionally, the big data market can be described as an economic space where data is collected, processed, analysed, and used to generate economic value. DLTs (e.g., blockchain) are not mandatory components of the big data production chain, but their use is important for ensuring transparency, security, and trustworthiness of data. These technologies enable new forms of digital trade in data and facilitate data exchange without centralised intermediaries, contributing to the formation of new economic relationships in the digital economy. It is important to consider the typology of data markets: on one hand, consumer-oriented markets imply individual ownership of personal data and direct participation in its monetisation. On the other hand, firm-oriented markets involve companies generating, owning, and using data, creating value, and engaging in data trade. Thus, access to data in digital markets has become a new dimension of competition. Such access often determines the limits of a company's innovation potential and the quality of service to consumers. When a company has exclusive access to large volumes of data, it may become a dominant player, increasing market concentration risks, restricting competition, and hindering innovation. Therefore, to assess a company's market potential, one must evaluate the technology enabling firms to build a big data ecosystem – particularly, access to the big data market and the architecture of big data, such as analysis of connectivity processes that define how data links within the ecosystem and its relevance in a domain ontology, i.e., the subject area of the data set, whether it is finance, healthcare, education, or others. According to the European Commission's guiding principles for digital ecosystems, the definition of a primary product market includes data from connected products, accompanying service data – the ancillary market – and processed data as the systemic market. Therefore, we can conclude that under EU regulation, the term "connected product" refers to the IoTs; the data collected by connected products is ancillary service data, and the processed data represents big data. When firms receive platform services, they also gain access to data. Data provides advantages to its holder. Accordingly, financial market actors seek to collect more data and analyse it better to gain a competitive edge. Data is considered a source of market power, while FinTech are multi-sided platforms forming complex ecosystems and acting as players in consumer-oriented data markets. Thus, FinTech participate in big data markets in dual roles – both in firm-oriented and consumer-oriented data markets. As such, potential competition focused on innovation should be taken into account when assessing a company's dominant market position. Defining the relevant big data market will help evaluate market structure and determine firms' market power.

Finally, the chapter examines the impact of big data on competition within the financial market, focusing on the evolving behaviour of digital financial actors and how they navigate a market driven by data access and digital tools. The chapter concludes by analysing how the growing influence of big data reshapes competition in the digital financial market, affecting both market structure and the strategic behaviour of market participants. It is noteworthy to clarify that in the competition model of data-driven companies, data is generated through consumers' economic activity and companies' investments in data infrastructure. Moreover, the sale of digital products depends on big data processing, further increasing the importance of information and communication technologies. Therefore, financial institutions are the most dependent on big data technologies and invest in order to process large consumer data sets using such technologies. With the help of multi-layered platforms, financial organisations collect, analyse, and develop better strategies using consumer data to attract more customers. They process data obtained from clients without restrictions, using automatic, semi-automatic, or manual tools. They obtain, collect, organise, store, and modify data – including large amounts of personal data – from the data subject or third parties. The more users there are, the more data is collected. Financial institutions rely on the feedback and monetisation loop. This loop gives companies the ability to gain data-driven market power even in adjacent markets. Therefore, financial market actors, specifically FinTech, seek to attract more users and increase access to consumer-oriented data markets, giving them a competitive advantage. Financial organisations acquire data through diverse methods – during client registration, from ready-made records, or by building an integrated service ecosystem from various sources and connected markets. Data acquisition is carried out at low cost. Financial institutions, by building private knowledge networks, control access to the data they acquire and prevent other companies from entering the market. Dominant companies in digital markets may restrict innovation and control prices. Thus, big data affects firms' competitiveness in developing and implementing innovation.

## Chapter VI
## Regulation of Big Data in Competition

Chapter VI addresses the regulation of big data within the framework of competitive digital financial markets, with a focus on how FinTech companies interact with big data to enhance their operations and services. It begins by examining the role of FinTech in the competitive landscape, exploring their integration into the business model of the financial sector and how big data contributes to their effectiveness in the banking industry. Moreover, it also highlights

the relationship between electronic money and electronic payments, analysing how these digital financial instruments are impacted by and operate within the broader context of big data. The chapter concludes with an analysis of the regulation of the digital financial market in the context of competition, focusing on the regulation of platform services and the information society. It examines how these digital platforms and financial sector actors are shaping and being shaped by regulatory frameworks in the digital financial market, offering insights into how competition is managed in this increasingly data-driven environment.

The financial sector is broad and includes various financial institutions. A financial institution is not a banking institution, although it is a credit institution that is limited in issuing certain types of credit and loans. A financial institution cannot issue electronic money, but it is a payment service provider and is limited in performing certain payment operations related to depositing or withdrawing cash from a payment account. Additionally, financial institutions are not involved in financial activities such as leasing, issuing guarantees, or trading in foreign currencies, interest rate instruments, or money market instruments. Therefore, financial institutions and banks operate under different functions and regulations, which also differently impact the FinTech they manage. It appears that, unlike financial institutions, banks have broader capabilities, can conduct more transactions, and are thus more dependent on large-scale data infrastructure than financial institutions. In Georgia, two major banks possess information about each other's clients, as their customer bases overlap. Consequently, in parallel with the development of FinTech, they are able to gain a comparative advantage in the market over both other financial institutions and banks. Together, the two banks hold significant personal data on clients who are also registered with other banks and can more easily collect data through digital channels, as the number of internet banking users continues to grow annually. It is noteworthy that the two large banks, by creating their own big data ecosystems through the development of FinTech that attract and process customer data using big data analytics, increase their efficiency and, therefore, their revenues.

Banks and their service platforms collect personal user data through various channels, including during registration, service usage, phone communication, branch visits, and through online services and platforms. They collect both identifiable personal information (such as name, surname, address, phone number, email, property and employment data) and behavioural data obtained through monitoring user activity (e.g., online behaviour, transaction history). During the electronic identification process, FinTech collect and process various levels of personal and biometric data for online authentication. Therefore, it is important to note that an IP address can also be considered personal data if it can be used to identify a person. Meanwhile, non-personal data, such as cookies, are widely used for user

behaviour analysis and platform optimisation. Banks use this data for analytics, which improves service quality and operational efficiency. Large sets of personal data processed by banks are stored in databases, and banks build "private knowledge networks." Accumulated data may be transferred to holding companies or third parties for specific purposes. Big data allows payment systems to better understand user behaviour, assess risks, and provide personalised services. The figures indicate the volume of transactions made by FinTech using electronic money and, consequently, the potential to generate big data. In the fintech industry, payments – especially internet and mobile payments – are one of the most important segments, as they enable financial transactions through advanced technology and promote e-commerce. In this context, payment service providers create software bridges between users and banks to ensure secure and automated transfers. It can be said that providers embed self-executing code in such software. Therefore, a smart contract can be considered a payment instrument when it is used to automate regular transfers. It represents a coded agreement between a provider and a user. Banks, as payment service providers, also use smart contracts to execute automatic transfers. They create electronic documents that have the same legal force as paper documents. Georgian legislation recognizes various forms of electronic payments (mobile, internet, etc.) as part of payment services, providing a legal framework for fintech services. Thus, it can be said that banks use smart contracts as payment instruments, while payment service providers use DLTs and smart contracts to become part of the big data ecosystem.

The second part of the chapter focuses on the intersection of big data and contracts in the digital market, addressing the practices of digital financial market agents and the responsibility they bear in using big data. It further explores crucial aspects of data security, detailing how financial institutions are expected to handle and protect data in compliance with legal and regulatory standards. Data security is of paramount importance – on the one hand, to protect confidentiality, since the law requires supervisory authorities to take appropriate measures to protect both entire data sets and their components or any configuration thereof. Given that data security is part of big data complex ecosystem, mechanisms for securing big data are integrated into the ecosystems used by companies. In conclusion, any connection established for the exchange and acquisition of data already forms part of the big data ecosystem.

The digital transformation of financial markets and the commodification of financial data present significant challenges for regulators and practitioners. The functioning of private blockchains relies on rules set by access gatekeepers, which influence data flow control and the capabilities of the fintech sector. The primary focus regarding financial data protection is confidentiality, but this is not sufficient. Financial information is a broad concept and is not clearly defined under Georgian legislation. FinTech companies can derive commercial benefits

by sharing financial data, but they often fall outside the scope of current regulations, posing a threat to data protection standards and consumer rights. It is noteworthy that EU legislation clearly defines the status and operational rules of different types of financial institutions, while Georgian law does not specify financial institutions, credit institutions, or other financial sector actors, complicating the creation of regulations and standards. The diverse nature of financial data requires broader and deeper regulation. The EU legal framework seeks to manage and standardise access to financial data. Existing legal frameworks (GDPR, PSD2) already include increased oversight of financial service providers. However, in practice, large technology companies often benefit most from new rules, as their human, technological, and financial resources allow them to use these regulations to maintain competitive advantages, leading to increased data concentration and reduced market competition. In regulating digital financial markets, it is necessary to take into account the new reality of free data flows and to expand regulations to ensure market efficiency, preserve competition, and maintain a level playing field for both traditional financial institutions and dominant tech firms.

The chapter also investigates the regulation of data in contractual relations within Georgia's digital financial markets, specifically discussing the contractual regulation of data exchange and the boundaries within which financial institutions are allowed to process client data. Georgian legislation does not define the concept or qualifications of a data access gatekeeper. Moreover, financial holding companies – under which multiple financial companies such as insurance firms, leasing companies, and banks operate – have the potential to develop FinTech that collect user data into a private data network. Therefore, such companies should be regulated with mechanisms like data access gatekeepers, ensuring that access to data is not made a mandatory condition for receiving services. This is particularly important given that banks and platforms may notify users that unless they agree to data access (e.g., cookies), they may not be able to use the services. It is also important to note that these same agreements describe the function of cookies as necessary for service improvement or automatic browser settings adjustment. Moreover, Georgian legislation requires that payment service providers have their head office located in Georgia, from where the actual business management is conducted. Consequently, financial institutions with branches in Georgia but without a head office in the country cannot be considered payment service providers and, therefore, cannot qualify as electronic money providers. Thus, legislation functioning as a data access gatekeeper will not apply to organisations without a head office in Georgia, such as PayPal, Revolut, etc.

## VII. Conclusion

The advancement of technology has significantly transformed society and business models, thereby underscoring the critical importance of data in the digital marketplace. In the digital economy, activities are conducted through the internet and digital technologies, which connect individuals, businesses, devices, data, and processes. Within modern business models, big data holds a central role. It refers to vast volumes of heterogeneous digital data – collected at high velocity from multiple sources and stored in raw form – whose processing requires advanced technologies and analytical algorithms. Big data may be structured, semi-structured, or unstructured. For companies, big data possesses economic value and thus practical utility. In the economy, big data is employed to foster innovation and to deliver targeted, updated, and improved products and services.

To leverage big data effectively, it is essential to establish both a data ecosystem and an appropriate data architecture that allow for rapid, real-time processing at minimal cost. A data ecosystem is a specialised form of digital ecosystem that brings together data owners (holders), analytics firms, professionals and researchers, cloud-service providers, and both commercial and academic institutions. This integrated infrastructure supports the collection, storage, analysis, and use of data. Data architecture – an integral part of the data ecosystem – defines data models, structures, and types; governs data throughout its lifecycle; and ensures security, quality, and integration, thereby underpinning decision-making aligned with organisational goals. Big data complex ecosystems rely on platforms that connect users with market actors. Companies store the data captured by these ecosystems in so-called Data Store Structures, then transform it into monetary value. Consequently, financial institutions in digital markets purchase cloud services such as software, platforms, and infrastructure, and build fintech platforms capable of aggregating massive datasets from various sources, thereby becoming part of the comprehensive big-data ecosystem. Under Georgian law, such ecosystems and architectures fall within the definition of "electronic means," encompassing devices used for data processing and storage. The legal definition of "information-society service" likewise includes platform services characterised by their digital delivery and remoteness. Thus, FinTech operates both as big-data ecosystems and as electronic intermediaries.

In turn, big data constitutes an intangible property asset, possessing both property and economic value. Its creation and utilisation require the expenditure of both material and intellectual resources. Big data can be bought and sold, transferred to third parties, either as cookies or as data collected and processed by the Internet of Things. This endows it with proprietary value in addition to its economic value. The property value of big data can be expressed in monetary terms; it generates material benefits and, as an intangible property asset,

serves as a source of law of things – it may be possessed, disposed of, and used, and it must be protected against unlawful interference so that its lawful owner can derive material benefits or acquire the right to claim against another person. To identify the proprietary value of big data, it is necessary to determine the methodology of its collection. Specifically, its collection and processing must involve a complex ecosystem and big data architecture. Big data is of significant proprietary value when it has economic value and practical utility. The acquisition, processing, and systematisation of big data require material and intellectual resources; consequently, the collected data should not have an exhausted life cycle and should be readily usable for business purposes. Through the processing and analysis of big data, it is possible to extract information.

Alongside digital services and digital infrastructure, platforms constitute one of the structural and integral components of the digital economy. A platform is a collection of markets through which services of the information society are delivered; by connecting market participants, such as service providers and consumers, it facilitates the provision of services via digital means. The regulation of competition in digital markets is primarily related to the gatekeepers of core platform services, which are deeply "embedded" within digital markets. Core platform services include online intermediation services, online search engines and social networks, video-sharing platforms, interpersonal online communication services, advertising services, and others. Digital markets, in turn, encompass a wide array of digital platforms characterised by diverse business models and attributes. Accordingly, there is no universal method for defining a relevant market in the digital economy that can be applied equally in all cases; the notion of the relevant market is inherently dynamic. Market definition requires the assessment of elements characteristic of the digital economy, including the identification of digital infrastructure, electronic commerce tools, and electronic intermediaries that connect consumers and suppliers, which may operate on either a paid or a free basis. In this context, the big data market constitutes an economic space: a collection of interdependent and technologically or technically interoperable production and value-creation chains. The big data ecosystem as a whole is itself a big data market, while its constituent elements form corresponding sub-markets. It may additionally be observed that in consumer-oriented big data markets, consumers own their personal data and participate directly in its monetisation. In firm-oriented markets, however, companies generate, own, and utilise data, create value, and engage in data trading. Access to data has thus become a new dimension of competition in digital markets. Such access often determines the limits of firms' innovativeness and the quality of the services they provide. Consequently, when a company enjoys exclusive access to vast volumes of data, it may emerge as a dominant market player,

increasing the risks of market concentration, restricting competition, and impeding innovative processes. Therefore, in assessing the market potential of companies, it is essential to evaluate the technologies that enable them to organise a big data ecosystem, in particular, access to the big data market and the architecture of big data. This includes analysing the connectivity processes that define how data are linked within the data ecosystem and domain ontology, specifically determining which segment of the semantic space the dataset pertains to, whether it is finance, healthcare, education, or another sector.

Financial sector service platforms collect customers' data through various channels, including during registration, service usage, telephone communication, branch visits, and via online services and platforms. FinTech companies gather both personal data and information obtained through the observation of user behaviour, as well as non-personal data, such as financial data, which are stored and processed by financial institutions in the ordinary course of their business activities. Georgian legislation does not fully regulate FinTech as big data ecosystems and service platforms; platform-based services are only regulated for financial organisations within the frameworks of cloud service models and information society services. In both cases, the primary objective of regulation is the protection of consumer rights. Therefore, the security of data collected by FinTech does not extend to the segment of non-personal data collection.

In the financial sector, banks, because of their function, offer the widest range of financial services to customers and, consequently, have greater opportunities as they are able to execute a larger volume of transactions. It is noteworthy that in the FinTech industry, payments – particularly internet and mobile payments – constitute one of the most important segments. Payment service providers create software-based connections between customers and banks to enable secure and automated transfers. Within these systems, providers integrate self-executing codes, turning smart contracts into payment instruments for the automation of regular transfers. Banks, as payment service providers, also employ smart contracts to execute automatic transfers. As a result, banks possess greater capacity than other participants in the financial sector to collect big data generated during the formation, execution, enforcement, and operation of digital contracts. The big data processed in banks are stored in databases, allowing banks to create "private knowledge networks." By establishing such "private knowledge networks," banks control access to the data they acquire and prevent other companies from entering the market. It is significant that in Georgia, two major banks hold information on the vast majority of clients in the banking sector. Thus, in parallel with the development of FinTech, banks have the opportunity to gain a comparative advantage in the market over other financial organisations as well as other banks. This advantage arises from

their easier access to data through digital channels and their ability to establish proprietary big data ecosystems. By developing FinTech solutions that both attract customers and process the data they generate through big data analytics, banks increase their operational efficiency and, consequently, their revenues.

Technological progress facilitates the large-scale collection of data but simultaneously increases security risks. Data security has immense importance: on the one hand, for the protection of confidentiality, as the law requires controllers to adopt appropriate measures to safeguard not only the integrity of information as a whole but also any part or configuration of its constituent elements. Since data security forms an integral part of the bih data complex ecosystem, big data security mechanisms are integrated into the complex ecosystems employed by companies. One of the tools for ensuring data security is distributed ledger technologies. Although they are not a mandatory component of the big data production chain, they enhance the transparency, security, and reliability of data. With respect to the protection of financial data, the primary focus is placed on confidentiality; however, this alone is insufficient, as the diverse nature of financial data requires broader and more in-depth regulation. The European Union's legal framework seeks to manage and standardise access to financial data. Existing regulatory frameworks (such as the GDPR and PSD2) already provide for enhanced oversight of financial service providers. In practice, however, large technology companies often benefit from the new rules, as their human, technological, and financial resources allow them to leverage the regulations to maintain their competitive advantage. In the process of regulating digital financial markets, it is essential to take into account the new reality of the free flow of data and to expand regulations to ensure market efficiency, preserve competition, and maintain a level playing field for both traditional financial institutions and technology firms occupying dominant positions. Accordingly, the protection of information requires the implementation of security systems founded on the principles of confidentiality, data integrity, and protection against unauthorised access. Moreover, in the context of international data transfers, data must be transmitted only to jurisdictions with high standards of personal data protection. In this regard, Georgian legislation also mirrors EU standards in the regulation of data transfers to other states or international organisations.

In turn, platforms that operate on a global scale and are not confined by state borders process personal data and transfer it to third parties within the framework of entrepreneurial activities. Consequently, data security is one of their primary objectives. As noted, appropriate measures must be taken by those who control the data to safeguard information as a whole, as well as any part of the information or any configuration of its constituent elements, all within the framework of confidentiality policies. Ensuring data security in any of the aforementioned

configurations also guarantees the protection of big data, whether it is structured, semi-structured, or unstructured, since it has been emphasised that any configuration of the constituent parts of information must be protected.

Georgian legislation does not recognise the existence or status of a gatekeeper. Moreover, when financial holding companies, under whose umbrella multiple financial entities operate (such as insurance companies, leasing firms, and banks), have the ability to develop FinTech that collects registered users' data within a private data network, thus, it becomes necessary to consider appropriate regulations. For such holding companies, it is advisable to establish regulatory measures ensuring that access to unnecessary data by financial service providers acting as gatekeepers does not become a prerequisite for the delivery of services. This is necessary to prevent gatekeepers from using non-personal data collected through FinTech platforms, which is obtained in the course of providing "platform-as-a-service" and performing the role of a financial intermediary. Such data are collected indirectly by the FinTech as users of the FinTech collect these data as part of their business activities while utilising the FinTech as part of their business activity. As discussed above, there are instances when a bank or platform notifies users that if they do not allow access to cookie files, they may be unable to use its services. It is noteworthy that the same agreements often define the function of cookies as procedures aimed at service improvement or at the automatic customisation of browser settings. Accordingly, the user should independently decide whether they need or not automatic browser customisation when using a FinTech service.

As noted, a trusted data ecosystem – particularly the presence of mechanisms ensuring data security and confidentiality – enables the extraction of value from big data. Consequently, the lack of protection renders big data valueless. In order to protect information derived from big data, it is advisable to develop a Georgian law "On the Protection of Trade Secrets" (see Annex 1 and Annex 3), which would safeguard not only the big data complex ecosystem and big data architecture (process) but also information with potential economic value. Furthermore, to protect the big data ecosystem and big data architecture, it is important to establish a legal framework governing the use of cloud outsourcing services by financial institutions. Such a framework would regulate the responsibilities of cloud outsourcing service providers and financial institutions in cases of trade secret violations. Additionally, in the Law "On Electronic Commerce," platform-based services should be addressed in greater detail (see Annex 2 and Annex 3); specifically, the law should not be confined solely to fee-based services but must also encompass those services that, while not remunerated, nevertheless collect data on platform users.