ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

LEGAL REGULATION OF BIG DATA IN E-COMMERCE IN UZBEKISTAN: CURRENT STATE AND DEVELOPMENT PROSPECTS

Khakimov Asadbek
Tashkent State University of Law
The student of Master's degree Business Law
e-mail: asadbekkhakimov421@gmail.com

Abstract: This article analyzes the current state and future prospects of legal regulation of Big Data in e-commerce in Uzbekistan, emphasizing personal data protection, electronic commerce operations, and competition law. Recent legal reforms, particularly the Law "On Personal Data" (№. LRU-547, 2019), the Law "On Electronic Commerce" (№. LRU-792, 2022), and the Law "On Competition" (№. LRU-850, 2023), have established a comprehensive framework addressing data localization, electronic contracts, and anti-competitive practices. The analysis highlights practical challenges, including strict data localization rules and regulatory enforcement difficulties. The article offers recommendations for improving regulatory clarity, enhancing institutional capabilities, and aligning Uzbekistan's legislation more closely with international standards.

Keywords: Big Data, e-commerce, personal data protection, electronic commerce law, competition law, data localization, regulatory challenges, digital markets, legal framework, consumer protection.

Introduction

Big data in e-commerce refers to the large volumes of consumer and transaction data collected through online platforms. In Uzbekistan, the rapid growth of e-commerce has made big data both a valuable asset and a source of legal concern. In 2021, Uzbekistan's e-commerce market generated about $1.39 billion in revenue and is projected to grow nearly 19 % annually by 2025[1]. This boom is fueled by increased internet access and digital payments, but it also raises questions about personal data privacy, cybersecurity, and fair competition. The government of Uzbekistan has recognized that a strong legal framework is needed to regulate how big data is used in online commerce, to protect consumers' rights and ensure a level playing field for businesses.

Over the past few years, Uzbekistan has enacted and updated key legislation that shapes the big data landscape in e-commerce. **The Law "On Personal Data" (№. LRU-547, 2019)** provides the foundation for personal data protection in the country[2]. **The Law "On Electronic Commerce" (№. LRU-792, 2022)** modernizes the rules for online commercial transactions, including data handling in e-commerce[3]. And most recently, **the Law "On Competition" (№. LRU-850, 2023)** was introduced to address anti-competitive practices in the market, explicitly

[1] Uzbekistan – eCommerce https://www.trade.gov/country-commercial-guides/uzbekistan-ecommerce
[2] Data Protection Regulations in the Nation of Uzbekistan https://caseguard.com/articles/uzbekistan-reinforcing-the-privacy-rights-of-citizens/
[3] Uzbekistan adopts new Law on E-commerce — Uzbekistan News | DARYO.UZ https://daryo.uz/en/2022/09/30/uzbekistan-adopts-new-law-on-e-commerce

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

covering digital and online businesses[4]. These laws, alongside related regulations, form the current legal framework governing big data use in Uzbekistan's e-commerce sector.

This article examines the current state of legal regulation of big data in e-commerce in Uzbekistan and discusses development prospects. It focuses on how the **Personal Data Law**, **Electronic Commerce Law**, and **Competition Law** operate in practice, highlighting real examples of enforcement and challenges. Where relevant, international best practices are referenced to contextualize Uzbekistan's approach. The aim is to provide a clear, practical overview of the legal issues and future directions, rather than abstract theory, so that readers can easily grasp the main ideas and implications.

Personal Data Protection in E-Commerce

Protecting personal data is central to regulating big data in e-commerce. Uzbekistan's Law "On Personal Data" (LRU-547, adopted July 2, 2019) is the primary legislation that governs the processing and protection of personal data[5]. This law was enacted to modernize data protection standards, replacing older, outdated provisions that dated back to the 1990s[6]. Under the Personal Data Law, **personal data** is broadly defined as any information recorded on electronic, paper, or other tangible media related to an identified or identifiable individual[7]. Rather than using the typical international terms "controller" and "processor" the law refers to an **"owner of a database"** (the entity that owns, uses, and manages a personal data collection) and an **"operator"** (the entity that processes the data on behalf of the owner). These terminology differences aside, the essence is that anyone collecting or handling personal information in Uzbekistan must follow certain principles and obligations.

The Personal Data Law lays down fundamental **data protection principles** that echo global standards – such as legality, accuracy, confidentiality, and security of personal data processing. Database owners and operators are required to ensure that personal data is collected and used for legitimate, specific purposes and is not excessive for those purposes. They must also take measures to keep data accurate and up-to-date, provide information to individuals about the processing of their data upon request, and delete or destroy personal data once the processing purpose is achieved or if the individual withdraws consent. These obligations mean that e-commerce businesses in Uzbekistan – which naturally gather a lot of customer data (names, contact info, purchase history, etc.) – have to implement proper data management practices. For example, an online retailer must not collect more personal information than necessary for a transaction and should secure the data from unauthorized access.

Notably, Uzbekistan's Personal Data Law was strengthened in **2021 with a data localization requirement** that has significant implications for big data in e-commerce. An amendment (Article 27[1] of the law) introduced in January 2021 mandates that personal data of

[4] Uzbekistan introduces a new legal framework to govern competition within commodity and financial markets (Detail) - Kinstellar https://www.kinstellar.com/news-and-insights/detail/2440/uzbekistan-introduces-a-new-legal-framework-to-govern-competition-within-commodity-and-financial-markets

[5] Data Protection Regulations in the Nation of Uzbekistan https://caseguard.com/articles/uzbekistan-reinforcing-the-privacy-rights-of-citizens/

[6] Data Protection Regulations in the Nation of Uzbekistan https://caseguard.com/articles/uzbekistan-reinforcing-the-privacy-rights-of-citizens/

[7] Data Protection Regulations in the Nation of Uzbekistan https://caseguard.com/articles/uzbekistan-reinforcing-the-privacy-rights-of-citizens/

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Uzbek citizens **must be processed using technical means physically located on the territory of Uzbekistan and in databases registered in Uzbekistan**[8]. In effect, this is a data localization rule: e-commerce platforms and other online services are obliged to store Uzbek consumers' personal data on servers within the country. Cross-border transfer of personal data is only allowed to countries that provide adequate data protection (a list of which has not yet been defined by regulators) or in certain exceptional cases such as with the individual's explicit consent[9]. The intent behind this localization measure is to assert sovereignty over citizens' data and ensure it remains under local jurisdiction. For instance, if a global e-commerce company operates in Uzbekistan, it should house the customer database on Uzbek soil or else face legal consequences.

Enforcement of the Personal Data Law, particularly the localization requirement, has been a challenge. Initially, authorities adopted a strict stance. In April 2021, soon after the localization rules took effect, the state communications regulator (Uzkomnazorat) took action against several foreign internet companies that were not complying. This culminated in **July–November 2021 incidents where access to major social networks and messaging platforms was restricted** for failing to localize Uzbek users' data[10]. On November 3, 2021, for example, **Uzbekistan temporarily blocked almost all major social media and instant messaging services** – including platforms like Facebook, Instagram, LinkedIn, and Telegram – on grounds that they violated the Personal Data Law's storage requirements[11]. The disruptions lasted several hours and reportedly caused millions of dollars in losses to businesses that rely on those platforms. This aggressive enforcement move provoked public criticism and highlighted the tension between enforcing data sovereignty and maintaining connectivity for citizens and businesses.

After that episode, the government appeared to recalibrate its approach. Several officials responsible for the earlier enforcement were dismissed, and the strict localization provisions **have not been aggressively enforced since late 2021 for most companies**. By August 2022, access to the previously blocked social networks was restored, and by January 2023 those platforms were largely unblocked for users. The only partial exception was reportedly TikTok, which remained under some restrictions, possibly due to ongoing data concerns. This sequence of events shows that while the law is on the books, its practical application is still evolving. Uzbek authorities faced a learning curve in finding the right balance: the initial crackdown underscored their commitment to data protection, but the economic ramifications made clear that an overly rigid approach could backfire.

That balance is now the subject of **reform and development**. In late 2024, the issue of data localization and its unintended consequences came to the forefront in high-level

[8] Uzbekistan: New Requirements for Uzbek Citizens' Personal Data Localization Enter into Force | Library of Congress
https://www.loc.gov/item/global-legal-monitor/2021-05-07/uzbekistan-new-requirements-for-uzbek-citizens-personal-data-localization-enter-into-force

[9] Data Protection Laws of the World
https://www.dlapiperdataprotection.com/guide.pdf?c=U

[10] Uzbekistan - eCommerce
https://www.trade.gov/country-commercial-guides/uzbekistan-ecommerce

[11] Uzbekistan's data localization law hinders entry of Apple Pay and Google Pay
https://kun.uz/en/news/2024/12/26/uzbekistans-data-localization-law-hinders-entry-of-apple-pay-and-google-pay

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

discussions. At an open dialogue with entrepreneurs on December 20, 2024, President Shavkat Mirziyoyev acknowledged problems caused by the current data localization rules, especially for integrating international services like Apple Pay and Google Pay into Uzbekistan's financial system. Representatives from the business community argued that requiring all personal and banking data to be stored only on local servers was hindering modern payment technologies and other services. In response, the President agreed that a well-thought-out solution was needed and indicated that the legislation would be reviewed. Indeed, the Central Bank of Uzbekistan has confirmed that **negotiations with companies like Apple and Google revealed the need to amend the Personal Data Law** – specifically the localization provision – to allow these global payment platforms to operate effectively. As a result, by early 2025, work was underway to draft changes that could relax or clarify the data localization requirement, signaling a prospect for a more flexible approach in the near future.

Aside from localization, the Personal Data Law imposes penalties for misuse of personal data which are important for e-commerce operators to heed. Violations of data protection rules – such as unlawful collection, disclosure, or failure to safeguard personal data – can lead to **administrative fines and even criminal liability**. For a first offense, fines can range up to a few hundred US dollars (in equivalent Uzbek currency) for individuals or officials responsible[12]. Repeated or serious violations escalate the consequences: a repeat offender can face fines of around 50 base units (over $1,000) and other sanctions, and extreme cases (for example, a violation leading to grave consequences or done with malicious intent) can result in criminal penalties, including correctional labor or imprisonment for up to three years. This legal deterrent means that an e-commerce business which, say, leaks a large customer dataset or uses personal data in an unauthorized way could be prosecuted. However, public information on enforcement of these penalties is sparse – to date, there have been few high-profile cases of e-commerce companies in Uzbekistan being fined under the personal data law, possibly because the law is still relatively new and awareness is growing.

It is also worth noting that **other related laws complement personal data protection in the e-commerce context**. For instance, the Law "On Electronic Commerce" itself (discussed below) contains a provision that the terms of use of personal data in e-commerce transactions must be defined by agreement between the parties[13]. In practice, this means that online sellers and marketplaces should include clear privacy policies or data usage clauses in their user agreements, ensuring that customers know and agree to how their data will be used. Additionally, the **Law "On Advertisement"** was updated in 2022 to introduce anti-spam rules: any dissemination of advertisements via telecommunications networks (which would include SMS, email or messaging in the context of e-commerce) now requires prior consent from the recipient. This aligns with personal data principles by preventing unsolicited commercial messages – an important aspect when big data is used for targeted marketing. Together, these measures show that Uzbekistan's legal framework is moving toward a regime where personal data is collected and used in e-commerce under defined consent and purpose limitations, much

[12] Uzbekistan: New Requirements for Uzbek Citizens' Personal Data Localization Enter into Force | Library of Congress
https://www.loc.gov/item/global-legal-monitor/2021-05-07/uzbekistan-new-requirements-for-uzbek-citizens-personal-data-localization-enter-into-force/

[13] Data Protection Laws of the World
https://www.dlapiperdataprotection.com/guide.pdf?c=UZ

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

like international best practices, albeit with a uniquely strict stance on data localization (for now).

Electronic Commerce Law and Data Use

A cornerstone of regulating big data in online markets is having clear rules for electronic transactions themselves. Uzbekistan addressed this by overhauling its e-commerce legislation in 2022. The **Law "On Electronic Commerce" (№. LRU-792)** was signed by the President on September 29, 2022 as a new edition of the law, replacing the older e-commerce law that had been in force since 2004[14]. This update was part of the national "Digital Uzbekistan – 2030" strategy, reflecting the government's intent to create a modern legal environment for the digital economy. The new E-Commerce Law establishes the legal status of electronic transactions and the obligations of parties involved, which indirectly affects how big data is generated and handled in the e-commerce process.

Key definitions and scope: The law defines who is considered a participant in "electronic commerce." It broadly includes **sellers** (which can be legal entities or individual entrepreneurs engaged in selling goods, works, or services via electronic trading platforms, as well as self-employed persons doing the same) and **buyers/consumers** (individuals or entities purchasing via electronic means)[15]. By explicitly recognizing self-employed individuals as sellers on e-commerce platforms, the law brings a wide range of online commercial activities under its ambit – from large online marketplaces to individuals selling handmade products on a website. All these actors are now clearly subject to certain rules, which helps in regulating even the long tail of e-commerce where big data can originate (for example, data from many small sellers can still accumulate into "big data" on a large platform).

Formation of electronic contracts: The law provides that an e-commerce contract (for instance, the sale of a product online) is concluded by the parties agreeing to the terms via electronic communications. In practice, this could be as simple as a buyer clicking "I agree" or checking out on a website, which constitutes acceptance of the seller's offer. The law recognizes several forms of expressing consent: an electronic document signed with an electronic digital signature, an electronic message indicating acceptance, or even actions that imply consent as specified in an offer. Importantly, **electronic documents and messages are given the same legal force as traditional paper documents**, provided they meet the requirements (for example, a digital signature where needed). This legal equivalence ensures that data generated in the course of online transactions (order confirmations, electronic invoices, click-wrap agreements, etc.) is legally valid. It also means disputes or issues arising from e-commerce can rely on electronic records as evidence, which is critical for enforcement and consumer protection.

Payment and data implications: The E-Commerce Law addresses how payments can be made in online commerce, which is closely tied to data flows. It allows payments through various methods: cash (with electronic POS receipts to record it), transfers from bank accounts (including via online banking or payment apps), and **electronic money (e-wallets)[16]**. The law even permits **escrow services** in e-commerce – operators of trading platforms or payment

[14] Uzbekistan adopts new Law on E-commerce — Uzbekistan News | daryo.uz
https://daryo.uz/en/2022/09/30/uzbekistan-adopts-new-law-on-e-commerce
[15] Uzbekistan adopts the Law "On Electronic Commerce" in a new edition
https://gratanet.com/news/uzbekistan-adopts-the-law-on-electronic-commerce-in-a-new-edition
[16] Uzbekistan adopts new Law on E-commerce — Uzbekistan News | daryo.uz
https://daryo.uz/en/2022/09/30/uzbekistan-adopts-new-law-on-e-commerce

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

service providers can hold a buyer's payment in escrow until the buyer confirms receipt of goods. These provisions encourage secure transactions and build trust in online shopping. From a data perspective, each of these payment methods and escrow arrangements generate financial and personal data (transaction records, delivery addresses, etc.) that businesses must handle responsibly. By formalizing such mechanisms, the law indirectly mandates that e-commerce platforms collect certain data (for example, to issue electronic invoices or to manage an escrow, some personal data and transaction details must be recorded) and thus ensures that those data handling processes are governed by law.

Consumer rights and data: The law also enhances consumer protection in ways that intersect with data use. It specifies procedures for delivery of goods, return of defective goods, and refunds to buyers in e-commerce transactions. For instance, if a product bought online is found defective, the buyer has the right to a replacement or repair, or to return it and get a refund, just as in traditional trade. To implement these rights, e-commerce operators need to maintain clear records of transactions, which are essentially data – proof of purchase, warranty information, communications between buyer and seller, etc. Ensuring these records are kept and made accessible to resolve disputes is part of compliance. While the law itself addresses the transactional aspect, the Personal Data Law discussed earlier would require that any personal information in these records (like the buyer's name or address on an invoice) be protected and used only for legitimate purposes (like processing the return).

Crucially for big data regulation, **the E-Commerce Law explicitly references personal data protection**. It stipulates that the **terms of use of personal data in e-commerce trading must be mutually agreed by the participants** (i.e., between the consumer and the e-commerce operator). In practice, this typically means that an online store or platform should have a privacy policy or terms of service that the user consents to, detailing how the user's personal data will be collected, used, and possibly shared in the course of the transaction. This provision bridges the gap between the general Personal Data Law and the realities of e-commerce by ensuring transparency at the point of data collection. For example, a shopping website might include a clause that by creating an account or placing an order, the customer agrees to the use of their personal data for fulfilling the order and for other purposes like marketing **if** they give additional consent. Uzbekistan's e-commerce law thereby makes it clear that handling of personal information is part of the e-commerce contract, reinforcing that such data use is not a given right of businesses but something that must be disclosed and consented to.

Though the Law on Electronic Commerce is relatively new, steps are being taken to enforce its provisions and integrate it with other regulations. A recent development is the government's move to formally **register and monitor e-commerce operators**. In December 2024, the Cabinet of Ministers issued Resolution No. 885, which among other things, established that as of July 1, 2025, all e-commerce operators (platforms, aggregators, etc.) in Uzbekistan must **register as local legal entities** and operate under a notification-based regime[17]. Under these rules, e-commerce businesses have to comply with all relevant laws, including the E-Commerce Law, Personal Data Law, consumer protection, copyright, advertising, etc. They are also required to provide information to authorities upon request and maintain robust information systems for their services. While this is a broader e-commerce sector regulation, it reinforces the idea that compliance with data

[17] Uzbekistan Introduces New Rules for E-Commerce Platforms - The Times Of Central Asia https://timesca.com/uzbekistan-introduces-new-rules-for-e-commerce-platforms/

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

protection and other legal obligations is not optional. An online marketplace in Uzbekistan, for instance, will need to be able to demonstrate that it is following the rules – from having proper online contract formation processes to protecting user data and honoring consumer rights. Failure to do so could result in penalties or even loss of the right to operate.

In summary, Uzbekistan's Law on Electronic Commerce creates a **structured legal environment for digital transactions**. By validating electronic contracts and signatures, it legitimizes the data and records at the heart of e-commerce. By outlining roles (sellers, buyers, platform operators) and responsibilities (payments, deliveries, returns), it indirectly dictates what data needs to be managed in these processes. And by linking with the Personal Data Law – requiring agreement on data usage terms – it ensures that big data collected via e-commerce is handled with respect for user consent and privacy. Together, these measures aim to foster consumer confidence in online commerce, which is essential for the continued growth of the e-commerce sector in Uzbekistan.

Competition Law and Digital Markets

The rise of big data in e-commerce also has implications for market competition. Large e-commerce platforms can accumulate vast datasets on consumers and competitors, potentially giving them an outsized advantage and enabling anti-competitive behavior (for example, using data analytics to undercut competitors' prices or favoring their own products on a marketplace). Recognizing these risks, Uzbekistan has updated its antitrust framework to cover digital markets and big data-driven business models. The **Law "On Competition" (№. LRU-850)** was adopted on July 3, 2023 (effective October 4, 2023) as a comprehensive new edition of the competition law, replacing the previous law from 2012. This new Competition Law introduces several concepts and rules that directly or indirectly regulate how big data can be used by dominant e-commerce players.

One of the notable innovations in the 2023 Competition Law is the introduction of the concept of **"superior bargaining power"** alongside the traditional concept of a dominant market position[18]. Under the law, a company **does not have to be a formal monopoly to fall under scrutiny**. Even without controlling a majority of market share, if a company (or group of companies) is able to unilaterally influence market conditions – for instance, by setting terms that suppliers or customers cannot avoid, or leveraging data to lock in users – it could be deemed to have superior bargaining power. This concept is particularly relevant in digital markets where network effects and data control can make a platform very powerful even if there are competing services. For example, an e-commerce marketplace in Uzbekistan that, say, controls a critical mass of user data and thus can dictate terms to merchants (even if its market share is below 40%) might be considered as having superior bargaining power under the law's definition. This widens the scope of competition regulation to capture big data-rich companies that are not traditional monopolies.

The law continues to cover **dominant positions** as well, defining dominance in a way that includes having a large market share (generally 40% or more) or other conditions like lack of alternatives in the market. Importantly for e-commerce, the law explicitly mentions **digital platform operators** as being subject to certain competition rules, which is a clear nod to online marketplaces and tech companies. The Competition Law lays out a detailed list of **prohibited**

[18] Uzbekistan introduces a new legal framework to govern competition within commodity and financial markets (Detail) – Kinstellar https://www.kinstellar.com/news-and-insights/detail/2440/uzbekistan-introduces-a-new-legal-framework-to-govern-competition-within-commodity-and-financial-markets

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

behaviors for firms with a dominant position or superior bargaining power (including digital platforms) to prevent abuse of their market power. These prohibited anti-competitive practices include, for example:

- **Creating artificial shortages or otherwise limiting market supply** in order to drive up prices, to the detriment of consumers (e.g., a dominant e-commerce platform could theoretically manipulate which products are available or promoted to induce scarcity and higher prices – this is forbidden).
- **Causing harm to consumer rights**, such as restricting consumers' ability to purchase the quantity or quality of goods they need (a platform cannot deliberately make it hard for consumers to buy from competitors or impose inferior quality choices).
- **Setting monopoly high or monopoly low prices**, meaning excessively overcharging (price gouging) or underpricing (predatory pricing) to destroy competition. For instance, using big data analytics, a dominant online retailer might identify a competitor's popular product and drastically undercut the price using its deep resources – this could be seen as anti-competitive if done to eliminate the competitor.
- **Imposing unfair contractual conditions** not related to the subject of the contract. In an e-commerce context, this could be a platform requiring merchants to share their customer data or pay for unrelated services as a condition of accessing the platform – such tying or extra requirements are prohibited.
- **Discriminatory conditions** – treating equivalent trading partners unequally without justification. A digital marketplace, for example, should not unfairly algorithmically promote one seller's products over another's in exchange for extra fees "under the table," nor should it misuse data analytics to give its own affiliated products a better placement than independent sellers, as that could be deemed discriminatory.
- **Refusal to deal and market barriers** – unjustified refusal to supply or purchase, or creating barriers to entry for other businesses. A dominant online platform couldn't, for example, suddenly cut off a supplier without reason if that prevents them from accessing consumers, nor could it use its data dominance to block a new entrant (like by exclusivity deals or technical barriers).
- There are additional prohibitions listed in the law, including forcing buyers to buy unrelated goods ("tying") and violating regulated pricing rules, among others. Collectively, these rules ensure that if a company in Uzbekistan's digital economy gains a big data advantage and market power, it must not exploit these in ways that harm competitors or consumers.

What these competition rules mean in practice is that **large e-commerce and tech companies are now on notice**: scaling up using big data is legal, but abusing the resultant power is not. For example, if an e-commerce platform uses its troves of consumer data to identify trending products and then favors its own brand of those products in search results, edging out independent sellers, this could trigger investigation as an abuse of superior bargaining power (discriminatory conditions or unfair advantage). Likewise, if a dominant online retailer were to use personalized pricing (a big data application) to systematically undercut certain rivals only in regions where those rivals operate, regulators might view it as predatory pricing. Uzbekistan's competition law framework is now equipped to handle such scenarios, much as competition authorities in the EU or US have started scrutinizing Amazon, Google, and others for their data-driven market practices.

To enforce these provisions, the law also calls for the implementation of **antimonopoly compliance programs** in certain organizations. Specifically, businesses above a certain size or

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

those holding dominant positions (including relevant government bodies and state-owned enterprises) are required to establish internal compliance systems to prevent competition law violations. This means, for instance, a leading tech platform in Uzbekistan should ideally have an internal team or protocols to ensure that its use of data and dealings with other market participants do not break antitrust rules. Such compliance systems are common in Western companies and their introduction in Uzbek law indicates an adoption of international best practices in regulatory compliance.

Since the law came into force in October 2023, there have not yet been publicized cases specific to e-commerce or big data-driven anti-competitive conduct, which is not surprising given the short time frame. However, the Competition Committee (sometimes referred to as the Antimonopoly Committee) is expected to issue guidelines and actively monitor sectors including digital markets. In 2024, the government also adopted subsidiary regulations to implement the Competition Law (for example, clarifying merger notification thresholds and procedures)[19]. These include oversight of acquisitions in the tech sector – a recognition that big data companies merging can also affect competition. Looking forward, if the e-commerce market continues to grow rapidly (with players like **Uzum** – a large local e-commerce ecosystem – expanding services, and foreign players like AliExpress or Wildberries present[20]), the competition authority will likely pay close attention. Any complaints by merchants or consumers about unfair practices could test the new law's provisions. For example, should a merchant allege that a marketplace misused sales data to launch a competing product and then pushed the merchant out, that could become a landmark case under Article 13 of the Competition Law (which covers abuse of dominance/superior power).

In essence, Uzbekistan's updated Competition Law brings its e-commerce and big data giants under regulatory oversight similar to global trends. It sends a message that **having a lot of data and market influence is acceptable, but abusing it is illegal**. This aligns Uzbekistan with international moves to keep digital markets competitive and fair, ensuring that innovation by new entrants is not squashed by data-rich incumbents and that consumers benefit from real competition.

Practical Challenges and Enforcement Issues

While Uzbekistan has put in place a comprehensive set of laws on paper, the practical reality of regulating big data in e-commerce comes with challenges. **Implementation and enforcement** are where the strength of these laws will ultimately be tested, and in Uzbekistan there have been both promising developments and clear obstacles in this regard.

One major challenge has been finding the right balance in **enforcing personal data protection without stifling the digital economy**. The 2021 social media blocking incident vividly demonstrated how heavy-handed enforcement of the data localization rule could disrupt the broader internet ecosystem[21]. The intention – protecting citizens' personal data – was laudable, but the method (suddenly blocking popular platforms) drew public backlash and harmed businesses that relied on those platforms for marketing and sales. It also put a spotlight

[19] Uzbekistan introduces a new legal framework to govern competition within commodity and financial markets (Detail) – Kinstellar https://www.kinstellar.com/news-and-insights/detail/2440/uzbekistan-introduces-a-new-legal-framework-to-govern-competition-within-commodity-and-financial-markets

[20] Uzbekistan – eCommerce https://www.trade.gov/country-commercial-guides/uzbekistan-ecommerce

[21] Uzbekistan's data localization law hinders entry of Apple Pay and Google Pay https://kun.uz/en/news/2024/12/26/uzbekistans-data-localization-law-hinders-entry-of-apple-pay-and-google-pay

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

on Uzbekistan in international media as a country with strict internet controls. In the aftermath, authorities walked a careful line: they did not repeal the localization law, but they quietly ceased its blanket enforcement for most of 2022 and 2023[22]. Essentially, the law remained in force but was not vigorously applied to foreign tech companies aside from warnings and symbolic fines. This kind of de facto moratorium suggests an understanding that sudden moves can have unintended economic consequences. However, the downside is that it creates uncertainty – companies are unsure if/when the law might be enforced again. Moving forward, one practical task is to clarify the localization policy, possibly by amending the law (as discussed in the prospects section) to avoid such disruptive enforcement swings.

Compliance costs and readiness are another practical issue. Data localization, for example, requires significant investment: companies must set up local servers or cloud storage within Uzbekistan and navigate a registration process for databases. Large international companies might afford it, but smaller foreign e-commerce sites or startups could be deterred from entering the Uzbek market due to these requirements. Even domestic businesses face costs to ensure data security and proper data handling protocols as mandated by law. Many Uzbek e-commerce entrepreneurs are tech-savvy but not all are well-versed in legal compliance – there is a learning curve to implement privacy policies, obtain user consents, and meet cybersecurity standards. The government has provided an online registry (the State Register of Personal Databases) and guidelines, but companies still need legal and IT expertise to fully comply. If compliance feels too burdensome, some might operate informally or ignore certain rules, which is counterproductive. Therefore, an ongoing challenge is to provide support (seminars, guidelines, perhaps incentives) to e-commerce businesses to comply with data protection laws in spirit, not just form.

On the competition front, a practical challenge is **monitoring and evidence-gathering** in the digital realm. Proving that a platform abused big data (for instance, an algorithm systematically giving its own products an advantage) requires technical investigation. The Antimonopoly Committee may need to develop new tools or collaborate with tech experts to detect anti-competitive algorithms or analyze large datasets for patterns. This is new territory for many regulators worldwide, not just in Uzbekistan. Additionally, because many digital platforms operate across borders, there may be jurisdictional issues when, say, a foreign-owned platform affects competition in Uzbekistan. The Competition Law does apply to foreign entities if their conduct affects Uzbek markets, but enforcing remedies on them might require international cooperation.

Judicial and regulatory capacity is an area for development. Uzbekistan's courts and regulators historically dealt with traditional commerce; now they must interpret and apply laws to complex digital scenarios. Training judges on data privacy rights or anti-monopoly cases involving tech will be crucial. Early enforcement actions will set precedents. For instance, if a consumer files a lawsuit under the Personal Data Law for misuse of their data by an online retailer, how the courts handle issues like calculating damages or assessing "consent" will shape future compliance. Similarly, if the Antimonopoly Committee investigates an e-commerce platform, the outcome will signal how strictly the law will be applied. So far, we have not seen public reports of major fines on e-commerce companies for personal data violations or competition infringements, which could indicate either good compliance or under-enforcement.

[22] Uzbekistan – eCommerce https://www.trade.gov/country-commercial-guides/uzbekistan-ecommerce

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Another challenge is keeping the **legal definitions up-to-date** with technology. Terms like "personal data" and even "electronic commerce" can evolve as new technologies (IoT devices, AI-driven services) emerge. For example, if e-commerce expands into the metaverse or via social media influencers collecting user data, the current laws might not explicitly cover those modes. Uzbekistan will need to continuously review and possibly amend laws or adopt new regulations to cover emerging big data uses (such as AI algorithms profiling consumers, or new forms of digital advertising and tracking). Already, the government has shown awareness by adopting recommendations on AI ethics, which is forward-looking. The challenge is to integrate such high-level principles into enforceable rules on the ground.

Cross-border data flows remain somewhat of a grey area for now. E-commerce inherently can be cross-border (Uzbek consumers buying on AliExpress, or local sellers reaching customers abroad). While the Personal Data Law restricts transfer to countries with "adequate" protection, it's unclear which countries qualify. Until Uzbekistan establishes a whitelist or clear criteria, companies face uncertainty about legally transferring data for, say, processing payments through foreign servers or customer support via international call centers. The risk is either over-compliance (firms refusing legitimate services because of fear of violating data transfer rules) or violation (sending data abroad regardless). This is an area where further guidance or bilateral agreements could help.

From a consumer perspective, **awareness and trust** are still developing. Many Uzbek consumers are relatively new to e-commerce and may not fully understand their data rights or the implications of big data. This could be a challenge because user vigilance can complement enforcement – if users know they have a right to opt out of marketing or to have their data deleted, they can demand it. If not, abuses might go unchecked. Government and civil society could play a role in educating consumers about privacy (for example, encouraging people to read privacy notices or be cautious about sharing personal information online). The introduction of requirements like opt-in consent for advertising messages is a positive step, but only if consumers utilize these rights (such as not giving consent when they don't want solicitations, or reporting spam if it occurs).

Finally, the sheer pace of e-commerce growth can be challenging for regulators to keep up. Uzbekistan's digital marketplace is expanding with local ecosystems and foreign platforms in the mix. As new services (like ride-hailing, food delivery, fintech apps) proliferate, all generating and leveraging data, the regulatory bodies must stay agile. Coordination between agencies – the ICT Ministry (for e-commerce oversight), the Personal Data Authority (Uzkomnazorat), the Antimonopoly Committee, and others – needs to be smooth, so that there are no gaps or overlaps in regulation. A practical example would be a large online platform that violates both data privacy and competition rules; the agencies should ideally coordinate their investigation and not work at cross-purposes. Achieving this kind of regulatory harmony is an ongoing task.

In summary, Uzbekistan has made commendable progress in setting up legal norms for big data in e-commerce, but **translating law into practice is an evolving process**. The country has already learned some lessons (as with the data localization enforcement) and is adjusting. Ensuring compliance without discouraging e-commerce innovation, building technical capacity for oversight, and keeping laws nimble for new tech are the main practical hurdles. How Uzbekistan navigates these in the coming years will determine how effective its regulation of big data in e-commerce truly is.

International Context and Comparative Perspectives

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

While focusing on Uzbekistan, it is useful to briefly consider how its approach to big data regulation in e-commerce compares to international best practices. Uzbekistan's legal developments have not occurred in isolation; they reflect a broader global trend of grappling with data protection and digital economy issues, albeit with local adaptations.

Personal data protection: Globally, the European Union's General Data Protection Regulation (GDPR) has set a high standard for data privacy, influencing many countries to update their laws. Uzbekistan's 2019 Personal Data Law was part of this wave of new privacy legislation. It shares common principles with international norms – for example, requiring lawful and consensual processing of personal information and obligating data handlers to ensure confidentiality and security. However, Uzbekistan's law also took a notably **sovereigntist turn with its data localization clause**, a feature more commonly seen in countries like Russia or China rather than in Western jurisdictions. The idea of mandating local storage of citizens' data is not a GDPR requirement (the GDPR focuses on safeguarding data and controlling exports, but not necessarily localizing it). In fact, the EU tends to promote cross-border data flows with protection. Thus, Uzbekistan's strict localization (Article 27^1) stands out in the international context. It prioritizes national control over data – which can enhance security and government oversight – but at the cost of erecting a barrier to the global free flow of data. Many countries in Central Asia and beyond are watching how this plays out: if Uzbekistan manages to revise this requirement to be more flexible (as current discussions suggest it might), it could align more closely with international practice that seeks a balance between open data exchange and privacy guarantees.

Electronic commerce laws: Uzbekistan's new E-Commerce Law aligns with widely accepted models, such as the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures. By recognizing electronic contracts and giving legal effect to digital communications, Uzbekistan is following the path many countries have taken to remove legal uncertainties in e-commerce. The emphasis on equal validity of electronic and paper documents is standard in international commerce now. Additionally, allowing for things like electronic payments and escrow services shows that Uzbekistan's legislation is keeping pace with e-commerce innovations, much like other countries that have updated their laws to accommodate fintech and online consumer protections. Regionally, countries such as Kazakhstan and Russia have also updated e-commerce and digital transaction laws in recent years; Uzbekistan's law is comparable in that it aims to facilitate online business while setting guardrails. One can say Uzbekistan's e-commerce law is broadly in line with **international best practices for digital trade facilitation**, which should make it easier for foreign companies to operate in Uzbekistan (knowing that electronic documents are recognized, for instance) and for Uzbek businesses to connect with global platforms.

Data in competition law: Internationally, there's a clear movement to address the power of big tech and big data in markets. The EU's approach has evolved through landmark cases (like the European Commission's actions against Google and others) and new regulations like the Digital Markets Act, which imposes ex ante rules on large "gatekeeper" platforms. The United States, while still relying on antitrust litigation, has seen cases challenging tech giants on how they use data to maintain dominance. In this global context, Uzbekistan's new Competition Law is a step in the right direction. By explicitly including digital platform operators and introducing the concept of superior bargaining power, it mirrors the concerns seen elsewhere: that even without monopoly, digital players can exert outsized influence. Not many countries

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

have the "superior bargaining power" concept codified; it appears in some jurisdictions (for example, Turkey's and Germany's competition laws have analogous ideas for supermarkets or tech platforms). Uzbekistan adopting it in 2023 suggests it is drawing from global discussions on how to rein in powerful companies before they become full monopolies. This is a forward-leaning stance consistent with best practices, aiming to prevent anti-competitive harm early. Moreover, the laundry list of prohibited abuses in Uzbekistan's law resembles provisions found in EU competition decisions or proposed legislation (like banning self-preferencing, unfair contract terms, etc.). Essentially, Uzbekistan is aligning itself with the international consensus that **big data should not be allowed to become a tool for anti-competitive conduct**, and it is arming its regulators with legal tools similar to those being considered or implemented in more advanced digital economies.

Another international angle is **cooperation and treaties**. Uzbekistan is not currently part of something like the Council of Europe's Convention 108 (a treaty on data protection) or other international privacy agreements, but it has shown interest in global frameworks. For instance, as noted earlier, Uzbekistan agreed to follow the UNESCO Recommendation on the Ethics of AI and a Global Data Security initiative. This shows an understanding that data issues cross borders. As e-commerce often involves cross-border transactions, Uzbekistan may in the future pursue mutual arrangements – for example, recognizing EU's GDPR adequacy, or bilateral deals with key trading partners – to facilitate data exchange while respecting privacy. In competition matters, international cooperation is also key: if a foreign company abuses dominance affecting Uzbek markets, the case might benefit from coordination with foreign regulators. While the Competition Law doesn't explicitly mention international cooperation, Uzbekistan could engage through networks like the CIS countries' antitrust coordination or even informal info-sharing with European or Asian competition authorities on cases of common interest.

In terms of **benchmarking**, one could say Uzbekistan's data privacy regime is more stringent in localization than international norms, but otherwise similar in principles to global standards (it provides for consent, individual rights, etc.). Its e-commerce regulation is standard and business-friendly, which is good for integration into the global digital economy. Its competition law is modern and on par with the kind of provisions that leading economies are instituting to address platform dominance. The main gap perhaps is enforcement experience and institutional strength, which will develop over time.

Overall, from an international perspective, Uzbekistan's efforts indicate a desire to catch up with and even preempt certain global regulatory trends. The country is effectively sending a message that it wants to harness the benefits of big data and e-commerce (as many nations do) but is also keen not to let those benefits come at the cost of personal privacy or market fairness. This balancing act is universally relevant, and Uzbekistan's journey – including its early aggressive stance on data localization and subsequent rethinking – offers a case study in how emerging digital markets try to find their own equilibrium in regulating big data.

Development Prospects and Recommendations

Uzbekistan's legal framework for big data in e-commerce is still evolving. Looking ahead, there are several areas where reforms and improvements are anticipated to better align the laws with practical needs and international standards. Here are the key development prospects and recommendations for the near future:

1. Refining the Personal Data Law (especially the localization requirement): The most pressing development on the horizon is a likely amendment of the data localization

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

mandate in the Personal Data Law. As discussed, by late 2024 Uzbek authorities were actively reviewing this provision due to its unintended consequences, like hindering the introduction of global payment services (Apple Pay, Google Pay)[23]. We can expect legislative changes that make the requirement more flexible – for instance, allowing personal data of Uzbek citizens to be stored or processed on foreign servers if certain conditions are met. These conditions could be: the foreign service adheres to strong data protection standards (perhaps an accreditation or certification process), or the data is stored in encrypted form accessible only in Uzbekistan, etc. Another approach could be shifting from a strict requirement to a preferential one (e.g., incentives for localizing data rather than an outright ban on foreign storage). The outcome of this reform will be crucial: it needs to maintain confidence in data security while opening the door for greater digital innovation and foreign investment. The expectation is that Uzbekistan will move closer to international practice by focusing on adequate protection of data rather than just its physical location. This would resolve the current limbo where the law says one thing but enforcement says another. It would also remove a significant friction point that currently exists for global e-commerce and tech companies considering operations in Uzbekistan.

2. Strengthening enforcement and oversight mechanisms: Enacting laws is only half the battle; enforcing them fairly and consistently is the other half. In the coming years, Uzbekistan is likely to invest in building the capacity of regulatory bodies like the State Inspectorate for Personal Data Protection (Uzkomnazorat) and the Antimonopoly Committee. This includes technical training, hiring specialists (for example, data analysts, IT auditors), and perhaps developing automated monitoring tools. For personal data, one recommendation is to introduce a clear **data breach notification requirement** and an incident response framework. Currently, if an e-commerce company suffers a data breach (say hackers steal customer information), it's not explicitly clear under Uzbek law what the company or authorities must do. Adopting such measures (common under GDPR and similar laws) would improve consumer protection and incentivize companies to improve cybersecurity. For competition, it might involve setting up a digital markets unit within the Antimonopoly Committee that continuously assesses the e-commerce landscape, similar to how some countries have dedicated tech regulation teams. Uzbekistan could also seek technical assistance and cooperation from more experienced jurisdictions. For example, the **Commercial Law Development Program (CLDP)** by the U.S. Department of Commerce and other international bodies have programs to help train regulators in emerging markets[24]. Engaging in such programs can accelerate the development of local expertise in handling big data issues.

3. Enhancing clarity through guidelines and secondary legislation: To help businesses comply, detailed guidelines can be issued. For instance, the government might publish a guide on "Data Protection in E-Commerce" that explains in practical terms how an online store should collect consent, how to implement the required security measures, how to handle cross-border orders, etc. Similarly, guidelines on what constitutes abuse of dominance in digital markets (with hypotheticals relevant to online platforms) could preemptively warn companies and educate stakeholders. In fact, the Competition Law empowers the authority to

[23] Uzbekistan's data localization law hinders entry of Apple Pay and Google Pay https://kun.uz/en/news/2024/12/26/uzbekistans-data-localization-law-hinders-entry-of-apple-pay-and-google-pay

[24] Uzbekistan | CLDP - Commercial Law Development Program https://cldp.doc.gov/category/countries-and-regions/central-asia/uzbekistan

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

issue regulations; these could define, for example, thresholds for what counts as "superior bargaining power" in various sectors, including maybe criteria like user base size, access to data, etc. If companies know the red lines, they can self-regulate better. An area in need of clarity is the definition of "adequate protection" for foreign countries under the Personal Data Law. Issuing a list of approved countries or a procedure for evaluation would help e-commerce businesses understand where they can lawfully send data (for cloud hosting, customer support, analytics, etc.). Until that is done, many may err on the side of caution or inadvertently violate the law.

4. Fostering international cooperation and data agreements: As Uzbekistan refines its laws, it could also pursue international arrangements to smooth data flows and enforcement. One prospect is seeking an "adequacy" decision from the European Union – essentially, having Uzbekistan's data protection regime recognized as equivalent to the EU's, which would greatly facilitate European companies doing business in Uzbekistan and vice versa. This is a long process and would require Uzbekistan to elevate certain standards (for example, possibly establishing an independent data protection authority, introducing rights like the right to be forgotten, etc., in line with GDPR). Nonetheless, it's a worthy long-term goal that would integrate Uzbekistan into the global data economy. In the interim, bilateral agreements, say with major trading partners or neighbors, about mutual recognition of data protection efforts or cooperation on cyber incidents could be beneficial. On competition, joining international networks such as the International Competition Network (ICN) or deepening ties within regional bodies (like Eurasian Economic Union if relevant, though Uzbekistan is not a member, or other CIS competition meetings) can help share knowledge on tackling big data cases. As global tech companies operate across countries, a coordinated approach can prevent them from exploiting regulatory gaps.

5. Keeping consumer rights at the center: Future developments should ensure that the end goal – protecting consumers and honest businesses – remains primary. For example, as e-commerce grows, Uzbekistan might consider strengthening its **consumer protection law** specifically for online transactions. While the E-Commerce Law and existing Consumer Rights Law already cover defective goods and such, new issues could be addressed: misuse of consumer data (which might be tackled by personal data law already), algorithmic transparency (perhaps requiring platforms to inform consumers if prices are personalized or if search results are sponsored), and dispute resolution mechanisms (like encouraging alternative online dispute resolution for e-commerce conflicts). Additionally, empowering consumer protection agencies or associations to take action when data abuses occur (like allowing them to file class-action suits or report issues to the data regulator) can improve enforcement from the grassroots. The more consumers trust that their data is safe and not being misused for shady practices, the more they will engage in e-commerce, which aligns with Uzbekistan's digital development goals.

6. Monitoring new trends and updating laws accordingly: Big data and e-commerce technologies evolve quickly – for instance, the rise of AI in customer service (chatbots collecting data), personalization algorithms, Internet of Things (IoT) devices in retail, etc. Uzbekistan will need to keep its laws under review. Already, by embracing AI ethics recommendations, the country shows foresight. We might see, in a few years, discussions in Uzbekistan about regulations on AI decision-making transparency or IoT data security. A proactive approach could be establishing a multi-stakeholder advisory group on the digital economy, comprising government, industry, tech experts, and academics, to continuously assess how well the laws are working and what new issues are emerging. This group could

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

suggest amendments to legislation before problems become acute. For example, if e-commerce platforms start using facial recognition for payments or in-store pickups, that raises biometric data issues that current law might not explicitly regulate – having a process to anticipate and address these through either new rules or clarifications will be important.

In essence, the development prospects for Uzbekistan's legal regulation of big data in e-commerce involve a combination of **legal amendments, capacity building, clearer guidance, and stakeholder collaboration**. The trajectory seems positive: the government is aware of the rough edges (like the need to fix the localization rule) and is keen to promote the digital economy which means they have incentive to improve the regulatory climate. If these recommendations are pursued, Uzbekistan could evolve towards a model where its data protection regime is robust but not restrictive, its e-commerce sector thrives under fair rules, and its competition watchdog effectively prevents the formation of data monopolies or unfair market practices.

Conclusion

Uzbekistan has made significant strides in establishing a legal framework to regulate big data in the e-commerce sector, reflecting a commitment to both foster digital economic growth and protect the rights of its citizens in the digital realm. Over the past few years, **new laws and amendments** – notably the Personal Data Protection Law (2019), the updated Electronic Commerce Law (2022), and the Competition Law (2023) – have addressed key aspects of data management, consumer protection, and market fairness in the context of online commerce. This marks a transition from a previously under-regulated space to one governed by clear rules. The current state of play is that online businesses in Uzbekistan must heed data privacy obligations (e.g. obtain user consent for data use and secure that data), follow proper procedures for electronic transactions, and refrain from anti-competitive conduct especially if they hold large market power through data advantages.

The **current legal regime** has brought Uzbekistan closer to international standards in many respects. Consumers now have legal assurances that their personal information should be handled lawfully and that they won't be spammed without consent. Online contracts and digital signatures are recognized, making e-commerce more secure and convenient. And the anti-monopoly rules guard against the kind of market abuses seen elsewhere when companies leverage big data to cement their dominance. Early enforcement actions, such as the 2021 crackdown on non-compliant social networks, underscored the government's resolve to uphold these laws. At the same time, those experiences also highlighted the need for **measured implementation** – too strict an approach can have economic downsides, whereas a calibrated strategy can encourage compliance while maintaining a healthy business environment.

Development prospects for Uzbekistan's big data regulation in e-commerce look promising, provided the momentum of improvement continues. As discussed, amending the data localization requirement will likely be a pivotal reform to watch in the near term, potentially opening doors for greater international integration and technology uptake. Strengthening institutional capacities – from better resourced regulators to informed judiciary – will be essential so that the laws on paper translate into effective protection and oversight on the ground. We can anticipate more guidance to help businesses understand and follow the rules, as well as greater public awareness efforts about data rights. Uzbekistan's willingness to adjust its policies (e.g., reconsidering Article 27^1 of the Personal Data Law) shows a pragmatic approach, focusing on outcomes rather than rigid positions.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

In conclusion, Uzbekistan stands as a **case study of a country rapidly updating its legal toolkit** to manage the double-edged sword of big data in e-commerce – leveraging data-driven innovation for economic progress while guarding against its potential to infringe on privacy and competition. The journey is ongoing: laws will continue to be refined in light of real-world outcomes and technological change. If the country strikes the right balance, it can look forward to a dynamic e-commerce sector where consumers feel safe and empowered, entrepreneurs can innovate with data responsibly, and market competition thrives. Achieving this balance will require vigilance and adaptability from lawmakers and regulators, but the foundation that has been laid is a strong one. By building on that foundation and learning from international best practices, Uzbekistan is well positioned to ensure that big data serves the public interest in the digital marketplace, rather than undermining it. The coming years will be crucial in translating the current legal promises into lived reality, thus fully realizing the development prospects of a secure and competitive e-commerce environment in Uzbekistan.

Sources:

1. Law of the Republic of Uzbekistan “On Personal Data” No. LRU-547 (2019)caseguard.comloc.gov (as amended 2021) and related regulations.
2. Law of the Republic of Uzbekistan “On Electronic Commerce” No. LRU-792 (2022)daryo.uzdlapiperdataprotection.com.
3. Law of the Republic of Uzbekistan “On Competition” No. LRU-850 (2023)kinstellar.comkinstellar.com.
4. Vakhidov & Partners, New Initiatives for the Advancement of E-Commerce in Uzbekistan (Legal 500, Feb 6, 2025)timesca.com.
5. Sadokat Jalolova, Uzbekistan Introduces New Rules for E-Commerce Platforms (The Times of Central Asia, Jan 6, 2025)timesca.com.
6. Dilshod Khabibullaev et al., Data Protection Laws of the World: Uzbekistan (DLA Piper, 2023)dlapiperdataprotection.comdlapiperdataprotection.com.
7. Global Legal Monitor: Uzbekistan – Personal Data Localization Enter into Force (Library of Congress, May 2021)loc.govloc.gov.
8. Kun.uz, Uzbekistan’s data localization law hinders entry of Apple Pay and Google Pay (Dec 26, 2024)kun.uzkun.uz.
9. U.S. Department of Commerce, Uzbekistan – eCommerce Country Commercial Guide (2023)trade.govtrade.gov.
10. Kinstellar, Uzbekistan introduces a new legal framework to govern competition... (Oct 2023)kinstellar.comkinstellar.com.
11. Daryo.uz, Uzbekistan adopts new Law on E-commerce (Sept 30, 2022)daryo.uzdaryo.uz.
12. Caseguard, Uzbekistan – Reinforcing the Privacy Rights of Citizens (Nov 2021)caseguard.comcaseguard.com.