OSCE ACADEMY in Bishkek

NUPI Norwegian Institute of International Affairs

POLICY BRIEF

#115

Data Access and Control in Young States: The Case of Kyrgyzstan

by Akylbek Dzhusupov

JULY
2026

This report became possible with financial support from the Norwegian Ministry of Foreign Affairs via the Academy's Cooperation with the Norwegian Institute of International Affairs.

OSCE ACADEMY in Bishkek
NUPI Norwegian Institute of International Affairs
POLICY BRIEF
115, JULY 2026

Data Access and Control in Young States: The Case of Kyrgyzstan

by Akylbek Dzhusupov

Executive summary

In the age of information and technology, vast amounts of data have become an asset to improving lives. At the same time, the large volume of data can present a major threat when in the hands of "bad actors." This is a particular risk when data is stored in a single location. As many governments struggle with how to appropriately control and ensure the security of large troves of data, it has become clear that limitations and guidance are necessary. This is especially true in countries where the governments themselves are likely to misuse sensitive data, and where there may be a tendency toward the establishment of "Data Dictatorship." Data Dictatorship describes the trend, seen especially among young states, of governments striving to collect all possible information about their citizens (regardless of physical location), visitors, and other persons deemed relevant to the country for governmental tracking and use. My research and recommendations, in this case focussed on the Kyrgyz Republic, serve to highlight that collecting this data in one place is dangerous.

Within this Policy Brief I compare the Kyrgyz Republic's current approaches with those which are practised in the European Union. Since EU law, values, and institutions share many commonalities with those of the Central Asian countries, EU law can serve as a role model, especially for Kyrgyzstan. I believe that such research into "Data Dictatorship" can help enhance human rights and strengthen the rule of law.

Akylbek Dzhusupov is a legal practitioner and PhD candidate at the Doctoral School of Law and Political Science at the Károli Gáspár University of the Reformed Church in Hungary. With nearly 20 years of experience in fintech, IT, banking, and corporate law, he has held senior legal positions in both private and state-owned banks in the Kyrgyz Republic. His research focuses on digital contracting, fintech regulation, economic integration, and the legal implications of digital transformation. Akylbek holds an LL.M. in International and European Business Law from Eötvös Loránd University and actively contributes to academic and policy discussions on digital economy governance and financial technology regulation.

E-mail: akyldzhusupov@gmail.com

Introduction

Data dictatorship (DD) refers to the practice of collecting, retaining, and using excessive, uncontrolled, and large-scale amounts of sensitive personal data, thus enabling authorities to exercise disproportionate power over individuals. Many countries continue to struggle with how to ensure that big data is secure and with regulations around the appropriate transfer of information to state bodies. This is especially true for non-democratic countries. Moreover, in most such cases the government itself misunderstands the value of sensitive data. Therefore, some information limits should be introduced to avoid the establishment of a "DicDATArship." While such rules should apply to all countries, they are particularly essential in young ones like the Kyrgyz Republic, where democratic governance is less well established. Governmental interests remain important, but they must always be balanced and justified – never assumed to automatically prevail.

The aim of this Policy Brief is to research the possible emergence of a DD in the Kyrgyz Republic and compare the current approaches of the country with those practiced in the European Union (EU), taken here as a standard for current best practice. There is also a strong historical precedent for EU law serving as a model for the Central Asian (CA) countries. For instance, the Public Fund Civil Internet Policy Initiative Study asserts that Kyrgyzstan clearly modelled its legislation on the EU's General Data Protection Regulation.[1]

[1] Ranking Digital Rights in Central Asia. *Public Fund Civil Internet Policy Initiative-CIPI* (2022): 11, https://rankingdigitalrights.org/wp-content/uploads/2023/05/CIPI-Central-Asia-report-May-2023.pdf

As the CA region and the EU have many common and similar values and institutions, the Kyrgyz Republic should be able to gain experience from EU practice. Thus, conducting DD research in such a manner may help enhance human rights and strengthen the rule of law in the CA region.

Attempts at Data Control

In 2018, a significant conflict emerged between commercial banking institutions and the State Financial Intelligence Service (the national anti-money laundering authority) of the Kyrgyz Republic regarding a request for the mass disclosure of all customer bank account information, including those of natural persons.[2] The banking sector's justification rested on the principle that the wholesale sharing of data violated constitutional principles, asserting that state access to information must be proportionate to the aim rather than encompassing all data, particularly concerning routine customers. While this occurred in 2018, the most severe attempts to put in place measures for accessing sensitive information were launched after the 2021 constitutional changes.[3]

This period marked the beginning of the strengthening of state institutions through the expansion of their powers, which granted them increased authority to process individual data. There were reports that the Kyrgyz government failed to respect restrictions on wiretaps, home searches, mail interception, and similar acts which were to be conducted only with the approval of the prosecutor and based on a court decision.[4]

On 3 April 2023, legislative changes expanded the power of tax authorities, granting them easier access to the banking information of private entrepreneurs and commercial companies, specifically during tax inspections.[5] However, for natural persons (individuals), the authorities

---

2 Maria Levina, "Kyrgyzstan: Commercial banks told to disclose information on customers," *The Times of Central Asia*, December 23, 2018, https://timesca.com/kyrgyzstan-commercial-banks-told-to-disclose-information-on-customers/#:~:text=The%20FIS%20actions%20are%20illegal%20and%20harmful,of%20bank%20secrecy%20and%20should%20be%20protected

3 Ayzirek Imanaliyeva, "Kyrgyzstan: Referendum hands Japarov the super-presidency he craved," *Eurasianet*, April 11, 2021, https://eurasianet.org/kyrgyzstan-referendum-hands-japarov-the-super-presidency-he-craved

4 Country Reports on Human Rights Practices: Kyrgyz Republic. *US Department of State* (2021), https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/kyrgyzstan/

5 The Law of the Kyrgyz Republic "On amendments to certain legislative acts of the Kyrgyz Republic in the field of taxation," *Ministry of Justice of the Kyrgyz Republic*, (April 3, 2023), https://cbd.minjust.gov.kg/112552/edition/1251787/kg

remained legally obliged to obtain a court order before accessing their personal account information. This differentiation was largely accepted by society, as it was perceived to be based on justified regulatory reasons. Nevertheless, this was followed by a push from government officials to secure even greater powers.

On 1 April 2024, the Ministry of Economy and Commerce of the Kyrgyz Republic initiated a public consultation process concerning a new draft law[6] focused on the provision of banking information to customs authorities. Specifically, the proposed legislation sought to mandate that all commercial banks must prepare and furnish data regarding bank transactions upon receiving a formal written request from the entitled organ of state customs. Articles describing the negative elements of this law were published in the academic literature and public discourse, and nothing appears to have come of the proposal.[7]

In July 2025, the Cabinet of Ministers of the Kyrgyz Republic launched a further legislative initiative aimed at securing sensitive individual data. This new bill proposed imposing an obligation on all banks and payment systems to automatically and regularly furnish data – without the requirement of an official request – pertaining to all individual money transfers exceeding a predetermined threshold. I drafted a comprehensive review[8] arguing for the abolition of this proposal, asserting that it not only constitutes a violation of existing law but also presents a significant strategic risk to both individuals and the stability of the state itself. Fortunately, the bill's authors publicly announced that they were excluding this "innovation" from the draft law. It was a local win, but the state representatives generally still do not understand the real threat of the "mass" flow of sensitive information. Consequently, there is a need for further research in this domain to persuade decision-makers that the centralized aggregation of big data concerning individuals constitutes a well-founded legal concern and a strategically dangerous practice.

---

6 The Draft Law on Amendments to the Law of the Kyrgyz Republic "On Banks and Banking Activities," *Unified portal for public discussions of regulatory draft legal acts of the Kyrgyz Republic*, (April 01, 2024), https://koomtalkuu.gov.kg/kg/view-npa/3635

7 Akylbek Dzhusupov, "Is banking secrecy under attack again?" *Banks portal*, (April 09, 2024), https://banks.kg/news/banking-secrecy-under-attack-again

8 Akylbek Dzhusupov, *LinkedIn*, "Review on Amendments to Tax Code of the KR (art. 146)," https://www.linkedin.com/posts/akylbek-dzhusupov-43115655_%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B2-%D0%BD%D0%B0%D0%BB%D0%BE%D0%B3%D0%BE%D0%B2%D1%8B%D0%B9-%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81-%D0%BA%D1%80-%D1%81%D1%82-146-activity-7358632915011874817-JhfR?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAuXG-UBKn5dmstHIT-BuzpT6aGlh6IjWLE

It is difficult to fully comprehend the ongoing escalation of practical and legislative measures being undertaken by the state to establish comprehensive control over all natural persons and to acquire detailed information about them.

For instance:

- The Government of the Kyrgyz Republic recently announced a monopoly over internet service in the country.[9] From now on the state-owned company will provide all internet service. This means that internet in the country will be under their full control;

- Recently, the state-owned bank bought shares in one of the biggest mobile communication companies.[10] Consequently, from among the three telecom companies of the country, two are under government control (Beeline and Mega). This also means the government controls the majority of communication in the country;

- The government has also introduced mandatory registration for all mobile devices with a state-owned company[11] founded by the state intelligence service.

There are many other amendments to laws which indicate that our young country is on its way to becoming a Data Dictatorship (or DicDATArship).

In the age of digitalization, when the state controls the internet, telecommunication, personal data, and financial operations, it gives the impression of total surveillance over every citizen of and visitor to the country. Such pervasive surveillance significantly undermines individual autonomy, making people feel compelled to conform to expected behaviour in public spaces.[12]

---

9 Turdubek Alymbaev, "Kyrgyzstan introduces temporary state monopoly on international Internet traffic," *24.kg News Agency,* July 29, 2025, https://24.kg/english/337806/

10 Emily J. Thompson "VEON Completes Sale of Beeline Kyrgyzstan," *Intellectia*, August 12, 2025, https://intellectia.ai/news/stock/veon-completes-sale-of-beeline-kyrgyzstan

11 Turdubek Aigyrov, "Mobile phones registration: State operator under SCNS oversight established," *24.kg News Agency*, August 08, 2025, https://24.kg/english/339002_Mobile_phones_registration_State_operator_under_SCNS_oversight_established/

12 Gizem Gültekin-Várkonyi, "Navigating data governance risks: Facial recognition in law enforcement under EU legislation," *Internet Policy Review* 13, no. 3, (September 2024): 10.

Furthermore, criminals, transnational digital companies and "rival countries" could also abuse the information stored by the authorities since there are no strict rules on information security for state bodies. Such potential abuse requires only that bad actors gain access to the information.

Overview of Kyrgyz Legislation

On 31 July 2025, the Digital Code of the Kyrgyz Republic[13] was adopted and replaced several earlier fragmented laws, including the Law on Personal Information (2008). This marks a major shift in the legal framework governing digital activities, including personal data protection in the Kyrgyz Republic. It is also important to mention that the Digital Code of the Kyrgyz Republic was the first introduced among Central Asian countries.

The Digital Code[14] consolidates and modernizes regulations related to personal data protection, digital services, telecommunications, artificial intelligence, digital ecosystems, and infrastructure. It introduces new definitions and responsibilities for personal data holders and personal data principals, digital resource owners, digital rights, digital ecosystems and the digital environment. The Digital Code continues to protect sensitive personal data and pays high attention to special categories of personal data, which include racial and ethnic information, political, religious and philosophical views, biometric and genetic data, health-related information, and gender and sexual orientation information.

Processing such data requires explicit consent, and there are strict rules for cross-border data transfers and automated decision-making. To best understand the intersection of sensitive information and specific state controlling powers under the Digital Code, you need to know the following:

---

13 "The President signed the Digital Code: how it will affect life in digital Kyrgyzstan," *Akchabar*, August 04, 2025, https://www.akchabar.kg/en/news/prezident-podpisal-tsifrovoj-kodeks-kak-on-povliyaet-na-zhizn-v-tsifrovom-kirgizstane-ldbzpqudrakifxxc

14 Digital Code of the Kyrgyz Republic, *Public Fund Civil Internet Policy Initiative*, (2025), https://internetpolicy.kg/wp-content/uploads/2025/10/Digital-Code-Of-The-Kyrgyz-Republic-.pdf

For Biometric data, in accordance with art. 48(3) of the Code "The following biometric data of the Kyrgyz Republic citizens shall be processed: digital graphic image of the face, graphic structure of the papillary patterns of fingers of both hands, handwritten signature."

For device control, according to art. 185(1) of the Digital Code "Mobile devices used to receive services in the networks of telecommunications operators of the Kyrgyz Republic shall be subject to mandatory registration in the state digital technological system for mobile device identification."

Regarding personal data, the Code establishes a modern and systematic framework for the regulation, enshrining fundamental principles of data processing (legality, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality), lawful grounds for such processing, and the rights of data subjects, while also providing for a designated competent public authority responsible for oversight in this domain. Nevertheless, notwithstanding the institutional presence of a regulator, the principal challenge lies not in the absence of, but in the insufficient elaboration on mechanisms for, effective implementation and enforcement. In particular, the broad formulation of legal grounds permitting processing without the consent of the data subject, as well as the specific regime applicable to public (governmental) services, creates a risk of expansive interpretation in practice, whereby the balance between public interests and individual rights may be shifted in favour of the state. Accordingly, the Digital Code may be characterized as a functionally coherent and conceptually sound legal framework; however, its effectiveness in ensuring the protection of personal data will largely depend on the quality of subordinate regulation and the development of consistent enforcement practice.

Moreover art. 130 of the Code significantly reinforces the digital ecosystem's privacy architecture by explicitly grounding the secrecy of digital correspondence and telephonic negotiations in constitutional and statutory law. This provision mandates that access to such data be restricted primarily to the original senders and recipients, while granting limited exceptions for service providers only when technically necessary for service provision. By requiring a specific judicial order for any third-party access – granted exclusively on an individual basis and for a designated duration – the point of the article is to prohibit arbitrary or mass surveillance, aligning with the core principles of data integrity and confidentiality established in the broader regulatory framework.

However, several law enforcement departments interpret the wording "access to secret data is permitted exclusively in accordance with statutory law" and push legislators to grant them power by adopting some specific laws. They believe that those laws are enough to ensure access to all forms of data constituting a secret. The individualized legal procedure mentioned in the Digital Code, however, ensures that privacy protections remain robust even when interacting with the broader requirements of public interest or law enforcement, thereby maintaining the legal hierarchy and transparency required to prevent the application of contradictory or unpublished regulations.

According to the Criminal Code of the Kyrgyz Republic (art 190), illegal collection, storage, use, and disclosure of confidential information concerning the private life of an individual without consent or legal basis provided for by law, are subject to a fine of 2500-6200 Euros or community service of 40–100 hours or correctional labour up to 1 year.[15] When it comes to sensitive financial information, the Law on Banks[16] is relevant. It establishes that any information that was provided by a customer to the bank or created by the bank, or otherwise arises in connection to the relationship between the bank and the customer (bank secrecy) is under protection and should be disclosed only upon the consent of the consumers. However, there are still a limited number of state authorities that have the right to access bank secrecy without the consent of the consumer:

- The financial intelligence agency in the field of combating the financing of terrorist activities and the legalization (laundering) of criminal proceeds;
- The tax body for the purposes of taxation;
- The credit bureaus in the field of exchanging credit information;
- The state notary offices on inheritance cases concerning the contributions of deceased depositors kept in their proceedings.

---

15 Graham Greenleaf and Tamar Kaldani, "Data privacy laws in Central Asia: between ex-SSR and 'Belt & Road'," *International Data Privacy Law* 15, no. 1, (February 2025): 67–90.

16 Law of the Kyrgyz Republic "On banks and banking" *National Bank of the Kyrgyz Republic,* (September 2022), https://www.nbkr.kg/index1.jsp?item=42&lang=ENG

Regrettably, in its decision dated 2 October 2024, the Constitutional Court[17] affirmed the legality of the tax authorities' actions pertaining to the mass acquisition of clients' financial transaction data, including those of natural persons. The Court based this justification on the asserted necessity of tax administration. Furthermore, the Court appears to have made a fundamental error in recognizing that the public interests may supersede the confidential well-being of citizens.

Additionally, the Law on the National Security Agencies of the Kyrgyz Republic[18] does not contain any regulations on how to request, collect, and store the personal data. Conversely, the Law on the Internal Affairs Agencies of the Kyrgyz Republic[19] contains the right to create and maintain databases in accordance with the procedure established by the personal information legislation of the Kyrgyz Republic, as well as electronic governance (art. 9(34)).

Best Practices from the European Union

1. European Union Legislation

We should start with the Charter of Fundamental Rights of the European Union (EU).[20] Under its art. 8, "personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." As civil rights, particularly the right to privacy, became more widely recognized, the European Data Protection Directive of 1995 (95/46/EC) was the first legal step to limit states' previously unrestricted data collection capabilities.[21] After two decades, this directive transformed to the well-

---

17 Decision on the constitutionality of subparagraphs a), b) of paragraph 1 of part 1, part 2 of Article 146 of the Tax Code of the Kyrgyz Republic, *Constitutional Court of the Kyrgyz Republic*, (October 2, 2024), https://constsot.kg/wp-content/uploads/2024/10/10-resh-ks-ot-02-10-24-russk.pdf

18 Law of the Kyrgyz Republic "On the national security agencies of the Kyrgyz Republic," *Ministry of Justice of the Kyrgyz Republic,* (July 2022), https://cbd.minjust.gov.kg/112389/edition/40023/ru

19 Law of the Kyrgyz Republic "On the internal affairs agencies of the Kyrgyz Republic," *Ministry of Justice of the Kyrgyz Republic,* (January 1994), https://cbd.minjust.gov.kg/686/edition/33628/kg

20 Charter of Fundamental Rights of the EU, *European Parliament* (December 18, 2000), OJ C 364/1, https://www.europarl.europa.eu/charter/pdf/text_en.pdf

21 Klaus Boers, Christian Grimme, He Huang, Stefanie Kemme, Marcus Schaerff, Tobias Singelnstein,

designed main law on personal data on the territory of the EU – the General Data Protection Regulation (GDPR).[22]

The EU legislators in the preamble mention that public authorities such as tax and customs authorities receive personal data which are necessary to carry out *a particular inquiry* in the general interest. This is the main point of difference compared to Kyrgyz law. The personal data can be received for particular cases, but not in order to search the data to create a particular case. This means that, before demanding personal data, authorities should initiate a case based on other information, and only then gain access to other relevant important information concerning the case such as personal data.

Another legislative act of the EU which regulates sensitive financial data is the PSD2.[23] There are some core articles linking PSD2 and GDPR obligations. In particular:

- Member States shall ensure that payment service providers only access, process, and retain personal data necessary for the provision of their payment services with the explicit consent of the payment service user (art. 94(1));

- The processing of personal data shall be carried out in accordance with Directive 95/46/EC (now GDPR) and Regulation (EU) 2016/679 (art. 94(2)).

The main point of the above-mentioned written rules is that government access to private data is not automatic and (1) must be prescribed by law, (2) necessary for a legitimate aim such as security or crime prevention, (3) proportionate to that aim, and (4) subject to judicial oversight. The handling of sensitive information must thus be purpose-specific and necessary, with robust legal safeguards, and individuals must be informed of the necessity of access and potential impact on their rights.[24]

"Social Control Through Data Science Systems: A Conceptual Essay," *International Criminology*, (December 29, 2025): 14-32.

22 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *European Parliament and Council*, (May 4, 2016), OJ L 119: 1–88.

23 Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *European Parliament and Council,* (December 23, 2015), OJ L 337: 35–127.

24 Klaus Boers, Christian Grimme, He Huang, Stefanie Kemme, Marcus Schaerff, Tobias Singelnstein, "Social Control Through Data Science Systems: A Conceptual Essay," *International Criminology*,

The EU also has an insightful e-Privacy Directive,[25] which applies to the processing of personal data in connection with the provision of publicly available electronic communication services in public networks. According to this directive, EU Member States must ensure through national laws that communications and related traffic data transmitted via public networks remain confidential by prohibiting any unauthorized interception, listening, storage, or surveillance, except when such actions are lawfully authorized or technically necessary to transmit the communication. Still EU Member States are allowed to limit certain privacy rights in electronic communications – such as the confidentiality of messages or limits on data processing, but only if they pass a law that is considered necessary, appropriate, and proportionate in a democratic society to protect important public interests such as national security, defence, public safety, or crime prevention.

2. European Union Case Law

EU case law, particularly the following cases of the Court of Justice of the EU (CJEU), provides a wide range of information and aids in understanding of the true values of a democratic society.

Case C594/12 (joined with C293/12, Digital Rights Ireland and Seitlinger and Others)[26]

This case marks a landmark ruling in EU data protection law. The main insight of the judgment is the declaration that the Data Retention Directive (Directive 2006/24/EC)[27] was invalid because it violated the fundamental rights to respect for private life and protection of personal data guaranteed by the EU Charter of Fundamental Rights.

(December 29, 2025): 14-32.

25 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *European Parliament and Council*, (July 31, 2002) OJ L 201: 37–47.

26 Court of Justice of the European Union. (2014). Digital Rights Ireland Ltd and Seitlinger and Others (Joined Cases C-293/12 & C-594/12). EU:C:2014: 238.

27 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *European Parliament and Council*, (April 13, 2006), OJ L 105.

The service provider collected excessive metadata such as date, time, duration and type of communication, identification of user's device and location thereof, the call recipient's number, and IP address. While such information provides a very detailed profile about an individual, it is not needed for the services provided.[28]

The CJEU ruled that the Directive, which required telecommunications providers to retain traffic and location data for all citizens for a minimum of six months and a maximum of two years, constituted an excessive and disproportionate interference with fundamental rights. The Directive was deemed invalid because it mandated the general and indiscriminate retention of data for practically the entire EU population, without requiring any connection between the data and a threat to public security. It lacked clear and precise rules governing the conditions for accessing the retained data by national authorities. Specifically, it did not require prior review by a court or an independent administrative body, nor did it establish objective criteria for limiting access to what was strictly necessary. The most significant insight of the ruling is the establishment of a strict proportionality test when EU legislation interferes with fundamental rights, particularly article 7 (Respect for Private and Family Life) and article 8 (Protection of Personal Data) of the Charter of Fundamental Rights of the European Union.

The Court articulated that:

- Retention of metadata is a serious issue: The data retained (location, time, duration, and recipient of communications) allows for "very precise conclusions to be drawn concerning the private lives" of individuals, including their daily habits, social relationships, and environments. Therefore, it constitutes a "wide-ranging and particularly serious interference."

- No general exceptions: While fighting serious crime is a legitimate public interest goal, the measures taken must be strictly necessary. The CJEU made it clear that a mass, untargeted surveillance measure like general data retention cannot be considered strictly necessary.

[28] Larisa Găbudeanu, Iulia Brici, Codruța Mare, Ioan Cosmin Mihai, and Mircea Constantin Șcheau, "Privacy Intrusiveness in Financial-Banking Fraud Detection" *Risks* 9, no. 6, (June 01, 2021): 104.

- Judicial safeguards are essential: Any future measure allowing public authorities to access retained data must be subject to rigorous procedural safeguards, including prior review by an independent body, to ensure the rights of the individuals concerned are protected against abuse.

This judgment set a high-water mark for data protection in the EU, forcing subsequent national data retention schemes to be far more targeted and subject to strict judicial oversight, a principle later reinforced in subsequent case law (e.g., the *Tele2* judgment, which is a landmark judgment that essentially affirmed and expanded on the principles).

Case C-203/15 and C-698/15 (Tele2 Sverige and Watson and Others)[29]

The CJEU ruled that national legislation providing for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users, relating to all means of electronic communication, is prohibited by EU law, specifically the e-Privacy Directive read in light of the fundamental rights to respect for private life (article 7) and protection of personal data (article 8) of the EU Charter of Fundamental Rights.[30]

The CJEU found that this kind of mass, untargeted retention of metadata constitutes a "particularly serious" interference with those fundamental rights.[31] The most critical insight is that the CJEU laid down a set of mandatory and stringent requirements that national authorities must meet to lawfully access retained communications data, even for the objective of fighting serious crime.

These include that:

- Access to retained data must be strictly limited to the objective of fighting serious crime (e.g., organized crime and terrorism), national security, or defence. Less serious objectives are

---

29 Court of Justice of the European Union. (2016). Tele2 Sverige AB v Post- och telestyrelsen, Case C-203/15, EU:C:2016:970.

30 Nina Gumzej, "Applicability of ePrivacy Directive to national data retention measures following invalidation of the Data Retention Directive," *Juridical Tribune* 11, no. 3, (December 2021): 430-451.

31 Xavier Tracol, "The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for a harmonised legal framework on the retention of data at EU level," *Computer Law & Security Review* 33, no. 4, (August 2017): 541-552.

generally insufficient to justify such an intrusion.

- While general and indiscriminate retention is banned, the CJEU specifies that targeted retention is possible as a preventive measure for fighting serious crime. However, this must be strictly limited to what is necessary in terms of the categories of data, the means of communication affected, the persons concerned, and the retention period.

- Access to retained data must, as a general rule, be subject to prior review by a court or an independent administrative authority. Exceptions are permitted only in cases of validly established urgency.

- The data must be retained within the EU to ensure that data protection rules are upheld.

- Affected persons should be notified of the access as soon as the notification is no longer likely to jeopardize the investigation.

In essence, the *Tele2/Watson* judgment confirms that data retention and access regimes must be targeted, proportionate, and subject to robust independent oversight, thereby severely restricting the ability of Member States to implement blanket surveillance measures in the digital realm.

Cases C-511/18 and C-512/18 (La Quadrature du Net and Others)[32]

These cases reiterate and refine the CJEU's strict position on data retention, clarifying that EU law generally prohibits the general and indiscriminate retention of traffic and location data, even for the purposes of safeguarding national security or combating terrorism.

Overall, these cases highlight that the CJEU confirms that national legislation requiring providers of electronic communications services to retain traffic and location data in a general and indiscriminate manner is incompatible with the e-Privacy Directive, read in light of the Charter of Fundamental Rights. This applies equally to measures taken for national security and those for combating crime.

[32] Court of Justice of the European Union. (2020). La Quadrature du Net and Others (Cases C-511/18 & C-512/18). EU:C:2020:791.

However, they also highlight that the CJEU identifies specific, narrow circumstances in which targeted or limited retention/access measures *are* permissible:

- General and indiscriminate retention: This is prohibited as a preventative measure.

- Targeted retention: This is permitted if strictly necessary to fight serious crime or prevent serious threats to public security, provided it is limited in time, geographically, and to specific categories of persons.

- General retention in exceptional circumstances: This is permitted only when the Member State faces a serious and genuine threat to national security that is present or foreseeable. Even then, it must be limited to a duration that is strictly necessary and subject to effective review by a court or independent administrative body.

The most significant insight of this judgment is the clarification that national security is not entirely outside the scope of EU law and judicial review, even though national security remains the sole responsibility of the Member States (as per Article 4(2) TEU).

The CJEU thus essentially sets the following critical safeguards:

- The e-Privacy Directive and the EU Charter of Fundamental Rights apply to national measures that impose obligations on electronic communications providers (private companies) to collect and retain data, even if the purpose is national security. This subjects such measures to the strict necessity and proportionality test.

- Any permitted retention or real-time collection measure, whether for fighting crime or for national security (including the use of automated analysis or "big data" tools), must be targeted and subject to prior review by an independent body, unless genuine urgency is established.

- There is a difference between the serious interference caused by retaining traffic and location data (prohibited generally) and the general and indiscriminate retention of civil identity data (such

as name, address, payment method), which is considered less intrusive and therefore permissible.

These rulings, once again, solidify the principle that mass surveillance regimes infringe on fundamental EU rights, demanding a shift toward targeted and legally constrained data practices, even for state security agencies.

Overall, the CJEU case law on large-scale surveillance of telecommunication data has evolved, whereby each judgment has been met with resistance by national governments and translated into their implementation of national data retention schemes.[33]

Conclusion & Recommendations

Based on an analysis of European Union best practices and an assessment of the current national legislative landscape, the following recommendations are proposed for implementation in the Kyrgyz Republic to mitigate the risks posed by the emergence of a Data Dictatorship.

- The mass acquisition, storage, and processing of sensitive personal data must be strictly prohibited by both legislation and judicial rulings unless it is tied to a targeted and specified case. Access to such sensitive information should only be granted to state bodies subsequent to the initiation of a concrete criminal or administrative proceeding.

- It also must be prohibited to impose an obligation on any private institution to routinely and indiscriminately provide comprehensive data pertaining to all of its customers initially collected for other purposes. This idea is supported by the European Union Agency for Fundamental Rights.[34]

---

33 Valsamis Mitsilegas, Elspeth Guild, Elif Kuskonmaz, and Niovi Vavoula, "Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks," *European Law Journal* 29, no. 1-2, (May 12, 2022): 176-211.

34 "Handbook on European data protection law: 2018 edition," *European Union Agency for Fundamental Rights,* (April 2018), https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

- All collected data must be retained only for the duration stipulated by national law. Upon reaching its expiry date, the data must be securely deleted prior to any public disclosure. The state should be obligated to publicly announce the date and time of this deletion process to afford interested parties an opportunity to observe the event. Furthermore, independent experts must be appointed to certify that the data has been irrevocably destroyed, precluding any possibility of restoration.

- The state should be legally required to create and maintain a comprehensive, publicly accessible register detailing the specific types of personal information collected by every state agency, department, and state-owned company. This register should specifically enumerate what kind of data is stored by a specific authority (personal activities, financial transactions, electronic communications (e.g., telephone and e-mail records), addresses, properties, GPS data, received services, purchased products, biometric data (e.g., images, voices), and behavioural profiles).

- The state must recognize that the practice of aggregating excessive volumes of data and centralizing its storage constitutes a significant systemic vulnerability, primarily presenting a threat to the state itself, and subsequently to individuals. Reliance on such massive, consolidated datasets creates the risk of catastrophic consequences should state systems, data centres, or essential infrastructure be compromised. The concentration of vast quantities of personal information significantly heightens the danger of a massive data breach, whereby criminals or other bad actors could gain unauthorized access to this critical information. Leaked data can be used to spam, bully, blackmail, cyberstalk, gain access to devices and identities, and/or to engage in criminal activity.[35]

[35] Ranking Digital Rights in Central Asia. *Public Fund Civil Internet Policy Initiative-CIPI* (2022): 11, https://rankingdigitalrights.org/wp-content/uploads/2023/05/CIPI-Central-Asia-report-May-2023.pdf

References

Aigyrov, Turdubek. Mobile phones registration: State operator under SCNS oversight established. *24.kg News Agency*, August 08, 2025. https://24.kg/english/339002_Mobile_phones_registration_State_operator_under_SCNS_oversight_established/

Akchabar, The President signed the Digital Code: how it will affect life in digital Kyrgyzstan. August 04, 2025. https://www.akchabar.kg/en/news/prezident-podpisal-tsifrovoj-kodeks-kak-on-povliyaet-na-zhizn-v-tsifrovom-kirgizstane-ldbzpqudrakifxxc

Alymbaev, Turdubek. Kyrgyzstan introduces temporary state monopoly on international Internet traffic. *24.kg News Agency*, July 29, 2025. https://24.kg/english/337806/

Boers, Klaus, Grimme, Christian, Huang, He, et al. (2025). Social Control Through Data Science Systems: A Conceptual Essay. *International Criminology* 6: 14-32. https://doi.org/10.1007/s43576-025-00204-1

Constitutional Court of the Kyrgyz Republic October 2, 2024. Decision on the constitutionality of subparagraphs a), b) of paragraph 1 of part 1, part 2 of Article 146 of the Tax Code of the Kyrgyz Republic. https://constsot.kg/wp-content/uploads/2024/10/10-resh-ks-ot-02-10-24-russk.pdf

Court of Justice of the European Union. (2014). Digital Rights Ireland Ltd and Seitlinger and Others (Joined Cases C-293/12 & C-594/12). EU:C:2014: 238.

Court of Justice of the European Union. (2020). La Quadrature du Net and Others (Cases C-511/18 & C-512/18). EU:C:2020:791.

Court of Justice of the European Union. (2016). Tele2 Sverige AB v Post- och telestyrelsen, Case C-203/15, EU:C:2016:970.

Digital code of the Kyrgyz Republic. https://internetpolicy.kg/wp-content/uploads/2025/10/Digital-Code-Of-The-Kyrgyz-Republic-.pdf

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the

protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002: 37–47.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). OJ L 337, 23.12.2015: 35–127.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. OJ L 105, 13.4.2006.

Dzhusupov, Akylbek T. Is banking secrecy under attack again? *Banks portal*, (April 04, 2024). https://banks.kg/news/banking-secrecy-under-attack-again

Dzhusupov, Akylbek T. Review on amendments to Tax Code of the KR (art. 146) [Post]. LinkedIn, August, 2025. https://www.linkedin.com/posts/akylbek-dzhusupov-43115655_%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B2-%D0%BD%D0%B0%D0%BB%D0%BE%D0%B3%D0%BE%D0%B2%D1%8B%D0%B9-%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81-%D0%BA%D1%80-%D1%81%D1%82-146-activity-7358632915011874817-JhfR?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAuXG-UBKn5dmstHIT-BuzpT6aGlh6IjWLE

European Parliament. Charter of Fundamental Rights of the EU. OJ C 364/1, 18.12.2000, https://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Union Agency for Fundamental Rights. Handbook on European data protection law. (2018), https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

Găbudeanu, Larisa, Brici, Iulia, Mare, Codruta, Mihai, Ioan Cosmin, and Șcheau, Mircea Constantin. Privacy Intrusiveness in Financial-Banking Fraud Detection. *Risks 9, no.*6 (2021): 104, https://doi.org/10.3390/risks9060104

Gültekin-Várkonyi, Gizem. Navigating data governance risks: Facial recognition in law enforcement under EU legislation. *Internet Policy Review* 13, no. 3 (2024), https://doi.org/10.14763/2024.3.1798

Greenleaf, Graham, Kaldani, Tamar. Data privacy laws in Central Asia: between ex-SSR and 'Belt & Road', *International Data Privacy Law* 15 no. 1 (2025): 67–90), https://doi.org/10.1093/idpl/ipaf001

Gumzej, Nina. Applicability of ePrivacy Directive to national data retention measures following invalidation of the Data Retention Directive. *Juridical Tribune* 11, no. 3 (2021): 431-451, https://doi.org/10.24818/TBJ/2021/11/3.02

Levina, Maria. Kyrgyzstan: Commercial banks told to disclose information on customers. The Times of Central Asia, December 23, 2018. https://timesca.com/kyrgyzstan-commercial-banks-told-to-disclose-information-on-customers/#:~:text=The%20FIS%20actions%20are%20illegal%20and%20harmful,of%20bank%20secrecy%20and%20should%20be%20protected

Mitsilegas, Valsamis, Guild, Elspeth, Kuskonmaz, Elif, and Vavoula, Niovi. Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal,* 29, no.1-2 (2023): 176-211, https://doi.org/10.1111/eulj.12417

National Bankk of the Kyrgyz Republic. Law of the Kyrgyz Republic on Banks and Banking. (September 2022). https://www.nbkr.kg/index1.jsp?item=42&lang=ENG

Public Fund Civil Internet Policy Initiative-CIPI. Ranking Digital Rights in Central Asia. (2022). https://rankingdigitalrights.org/wp-content/uploads/2023/05/CIPI-Central-Asia-report-May-2023.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. OJ L 119, 4.5.2016: 1–88.

Thompson, Emily J. VEON Completes Sale of Beeline Kyrgyzstan. *Intellectia*, August 12, 2025. https://intellectia.ai/news/stock/veon-completes-sale-of-beeline-kyrgyzstan

Tracol, Xavier. The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for

a harmonised legal framework on the retention of data at EU level. *Computer Law & Security Review* 33, no. 4 (2017): 549. https://doi.org/10.1016/j.clsr.2017.05.003

US Department of State. *Country Reports on Human Rights Practices: Kyrgyz Republic.* (2021). https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/kyrgyzstan/

OSCE Academy in Bishkek
1A, Botanichesky pereulok
Bishkek, Kyrgyz Republic 720044

Tel: +996 (312) 54-32-00, 54-12-00
E-mail: rtd@osce-academy.net
Website: www.osce-academy.net