E-justice and Cyber Security: Balancing between Openness of the Courts and Data Protection in Kyrgyzstan

Aliia Maralbaeva[1]

Introduction

The digital transformation of public services includes the implementation of e-justice (i.e., information and communication technologies [ICT] in the judicial system) in Kyrgyzstan. The e-justice systems, such as e-case management, audio-video recording of criminal proceedings, remote hearings via videoconference in court, an online portal for publicly available court decisions, and the e-portal "Digital Justice" facilitate transparency, efficiency, and accessibility, the openness of information connected with the courts, and the digitalization of court business processes and administration. At the same time, however, they significantly increase data storage and raise challenges and risks for privacy, confidentiality, and data security.

Kyrgyzstan signed the Universal Declaration of Human Rights and ratified the International Covenant on Civil and Political Rights, which guarantee a fundamental right to a fair trial, the right to public information, and the right to a public trial. The Constitution of the Kyrgyz Republic also contains similar provisions. According to part 3 of Article 33 of the Constitution, everyone will be guaranteed access to information under the jurisdiction of state bodies, local self-government bodies, and their officials. The procedure for providing information is to be determined by law. Part 1 of Article 100 of the Constitution stipulates that "all courts shall hear cases in public. A case may be heard in closed session only in cases provided for by law. The court judgment shall be announced publicly".[2] The transparency and openness of the courts are based on the aforementioned constitutional rights.

---

1 Aliia Maralbaeva (PhD) is a Volkswagen Foundation Postdoctoral Fellow (Germany) and Associate Professor of Law, Department of International and Business Law, Ala-Too International University (Kyrgyzstan).

2 The Constitution of the Kyrgyz Republic (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112213?cl=ru-ru.

In this chapter the word "transparency" means a mechanism that should be the result of a method of governing, administration, and management by the state that allows citizens control of and participation in public matters. In practice, this should include access to public information, the state's obligation to generate information and make it available to citizens in a manner that allows for broad access, and the empowerment of citizens to demand that the state comply with its obligations. Openness is an element of the transparency; it can be understood as the various manifestations of a proactive policy whereby relevant information is made available to the public (Herrero and López 2010: 9).

Since the implementation of e-justice systems in courts the concept of openness of the court has been changed. Eszter Bodnár (2016: 154) argues that today openness no longer means only the physical presence in the courtroom, but also includes an electronic aspect. Court websites become an effective tool for e-communication between the judiciary and citizens. The e-portal "Digital Justice" and website *act.sot.kg* provide access to a database of court judgments and judicial acts. The websites of the Constitutional Court, the Supreme Court, Bishkek city court and regional courts (*oblastnye sudi*) enable the public to learn about what they do and how they operate (through, e.g., calendars of court hearings on constitutional, criminal, civil, and administrative cases, an e-calculator of state duty, information about judges, samples of documents, an e-court application form for citizens and legal entities, the work schedule of the courts, and a timetable for the reception of citizens). Only the Constitutional Court publishes video recordings of court hearings. It also provides access to a database of court judgments and press releases regarding the cases on its website.

As a result of the relatively recent application of e-justice systems in Kyrgyzstan, the 2018 Information Security of the Judicial System Concept outlining the cyber security of e-justice has to be amended. In light of this gap, this chapter shows how to keep the balance between openness of the courts and data protection while using e-justice systems. The methodology for this research includes analysis of national legislation, government strategies, and implemented e-justice systems, and is complemented by a case study of 280 court judgments on domestic violence cases published online by district and appellate courts in Bishkek, the capital city, and in the regions between 2019 and 2021, the aim being to examine the impact of online publication of these judgments on the principle of openness of

courts and personal data protection, as well as an interview with a court clerk.

Analysis of the literature on the impact of e-justice systems on the openness of the courts, cyber security in the judicial system, and data protection reveals several approaches. Bodnár (2016) has argued that the transparency and openness of the judicial system are supported by the constitutional principle of legal certainty. Specifically, she has stated that "from this principle comes the requirement that the decisions should be published and available for analysis. Openness and transparency ensure that courts operate in a predictable and foreseeable manner, which contributes to legal certainty" (Bodnár 2016: 154). On the other hand, however, Peter Winn has emphasized the balance between the presumption of the openness of judicial proceedings and the privacy rights of litigants, witnesses, and other third parties that the court should maintain. In addition, he has stressed that "failure of the legal system to maintain the ancient balance between access and privacy will lead to the greatest danger of all – inhibiting citizens from participating in the public judicial system" (Winn 2004: 311). The study by Isam Faik and colleagues has revealed "the inherently equivocal nature of the role of ICTs in transformation towards more open forms of organizing the judicial system" (Faik 2019: 694). On the one hand, the introduction of ICTs into the judicial system can maintain and reinforce entrenched boundaries. On the other, it can constrain openness.

The chapter examines e-justice and cyber security and how they impact on the traditional balance courts have reached between the openness of proceedings and data protection for litigants, witnesses, and other third parties in the digital era, as well as providing recommendations on how to ensure balance between the openness of courts with respect to information and data protection in Kyrgyzstan by improving national legislation.

Architecture of e-justice in Kyrgyzstan: a brief outline

E-justice is an umbrella term that captures any effort to administer, deliver, strengthen, or monitor justice services using digital technologies. E-justice broadly covers all kinds of digital technologies from complex case management or innovative apps to information technologies and the use of online communication. It includes the tools and processes used by justice sector professionals and those used by the public and the media. E-justice initiatives include the strategies, process (re)engineering, automation, data

collection, and the integration of systems as well as online dispute resolution, e-filing, remote court process and technologies used to digitize, store and provide access to legal documents and evidence (UNDP 2022: 52).

In Kyrgyzstan, there are two main types of e-justice systems. First, e-justice systems that provide access only for authorized users such as judges, court clerks, prosecutors, investigators, bailiffs, and litigants. They comprise: (1) an e-case management automated information system (hereinafter AIS "Sud") which also includes automated allocation of cases, (2) audio-video recording of criminal proceedings, (3) remote hearings via videoconferencing, (4) the AIS "Unique Register of Crimes", (5) the AIS "Enforcement Proceedings", and (6) the AIS "Probation." These e-justice systems are intended to digitize business processes, provide access to audio-video recordings of criminal proceedings to parties and develop e-registries within the courts, prosecutors' offices, bailiff service units, and the probation department of the Ministry of Justice. They are not open to the public.

Second, e-justice systems that ensure openness of the courts for public access. They include: (1) an online database of court judgments (*act.sot.kg*), (2) websites of the Constitutional Court, Supreme Court and regional courts, (3) the e-portal "Digital Justice". The latter was introduced in 2023 and is now at the stage of active development. This e-portal is an umbrella that "brings together all types of services in the justice system and is designed to provide easier access to court for ordinary citizens," including access to a database of court judgments and acts, information about court hearings including the date, time, and place of the trial, as well as general access to judicial acts on the Internet resource of the Supreme Court. It allows open interaction with citizens, which allows them to file applications, lawsuits, and complaints with the court, as well as to perform other procedural actions in electronic format. Within the framework of the portal, it is planned to launch an online participation system for parties to court proceedings.[3]

In legal scholarship, the principle of openness of judicial proceedings is "limited when it interferes with the fair and impartial administration of justice, or threatens the safety or the reasonable expectation of privacy of the participants in the judicial process" (Winn 2004: 308). For this reason, it is necessary to determine the approach that could help to keep the

3 "Chief Justice of the Supreme Court: Kyrgyzstan will be able to achieve full transition to digital format and electronic court proceedings." Available online at: https://kg.akipress.org/news:2006245/?from=kgnews&place=maincats.

balance between openness of the courts and data protection of participants of proceedings.

E-justice and openness of the courts in the digital era: main findings

E-justice and Access to Information in Constitutional Proceedings

Bodnár has highlighted the importance of openness and transparency in cases of constitutional review. She has argued that "these decisions are taken in the political sphere, sometimes limiting the power of the two other branches, the legislative and executive branches"(Bodnár 2016: 155)

According to the Article 97 of the Constitution of the Kyrgyz Republic the power of constitutional review is vested in the Constitutional Court. Part 3 of Article 97 of the Constitution establishes that "Everyone shall have the right to challenge the constitutionality of a law and other normative legal acts if he or she believes that they violate the rights and freedoms recognized by the Constitution."[4]

The principle of openness of constitutional justice is embodied in Article 12 of the Constitutional Law "On the Constitutional Court of the Kyrgyz Republic", which guarantees public hearings by the Constitutional Court. "The court hearings are held in a courtroom accessible to representatives of civil society and mass media. Decisions of the Constitutional Court are proclaimed publicly."[5] At the same time, the presumption of openness is limited. Closed court hearings are allowed for the protection of state secrets, the safety of citizens, the privacy and the protection of public morals.[6] In other words, there is no general public right of access to the court when these types of hearings are in progress.

The e-justice system facilitates public access to the Constitutional Court and guarantees the principle of openness of proceedings. The Constitutional Court publishes the court judgments on its official website and press releases on cases. According to the Law of the Kyrgyz Republic "On Access to Information under the Jurisdiction of State Bodies and Local Self-Governance Bodies of the Kyrgyz Republic," the judgments and opinions of the

4 The Constitution of the Kyrgyz Republic (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112213?cl=ru-ru.

5 Constitutional Law "On the Constitutional Court of the Kyrgyz Republic" (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112318.

6 Ibid.

Constitutional Chamber of the Supreme Court of the Kyrgyz Republic[7] are fully published.[8]

At present, only the Constitutional Court provides public access to video recordings of proceedings on the official website and a Youtube channel. However, the Constitutional Court website is not adapted for people with disabilities. In this regard, Chyngyz Shergaziev (2023: 458) has highlighted that accessibility for people with disabilities contributes to openness of constitutional justice.

The Covid-19 pandemic had an impact on the digitalization of constitutional proceedings. In 2021 the new Constitutional Law of the Kyrgyz Republic "On the Constitutional Court of the Kyrgyz Republic" was adopted. It establishes online court hearings in certain cases in order to provide access to constitutional justice and ensure the principle of openness of the court.[9] However, the Constitutional Court does not conduct online court hearings yet (Shergaziev, 2023: 457).

Another type of e-justice system that provides access only for authorized users such as justices and court staff was implemented in the Constitutional Court with support of IDLO USAID in 2014. It is called an "Electronic Document Management System" (hereinafter EDMS). It was designed specifically for internal e-workflow within the Constitutional Chamber. According to new Constitutional Court Regulations adopted in 2022 "the list of applications accepted for proceedings and cases scheduled for court hearings are placed in EDMS".[10] Shergaziev has elaborated:

> EDMS [allows you] to fully automate the office workflow, reduce the time for processing documents and reduce the risks of accidental loss of data. All incoming and outgoing documents are stored in the system in PDF format, which are downloaded immediately after their registration. The EDMS function of monitoring the flow of documents and controlling their execution allows monitoring the workload of both judges and staff, which, in turn, facilitates the distribution of cases and

7 The Constitutional Chamber was a predecessor of the Constitutional Court, which was reestablished in 2021.

8 Law "On Access to Information under the Jurisdiction of State Bodies and Local Self-Governance Bodies of the Kyrgyz Republic" (2006), available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/202010.

9 Constitutional Law "On Constitutional Court of the Kyrgyz Republic, available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112318.

10 Constitutional Law "On Constitutional Court of the Kyrgyz Republic" (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112318.

> documents depending on their workload. For the convenience of judges and staff, a "Workroom" has been created where they can see up-to-date information on their workload, as well as on scheduled meeting dates. In addition, the EDMS has provided a wide range of possibilities for the output of statistical reports for analyses, which include summarized information on core subjects, regions of applications, on the progress of the execution of applications and complaints. (Shergaziev 2023: 456)

Since 2022, the Constitutional Court has also joined the automated electronic document management system "Infodocs" which allows digital interaction with other governmental bodies (Shergaziev 2023).

Overall, the e-justice system introduced in the Constitutional Court does contribute to the principle of openness of the court.

E-justice and Access to Information in Criminal Proceedings: The Case of Domestic Violence

For criminal proceedings, the principle of openness is embodied in Article 291 of Criminal Procedural Code, which guarantees a public trial. Nevertheless, the right to public trial is not absolute. The principle of openness of criminal proceedings is limited. There is no public access to closed trials, which are allowed:

> in cases when it may lead to disclosure of information constituting a state or other secret protected by law; in cases of offences against sexual inviolability and sexual freedom of the person, and other crimes in order not to disclose information about intimate aspects of the life of participants in proceedings or information degrading their honor and dignity; in the case of criminal cases involving offences committed by children under 16 years of age; in cases where this is required in the interests of safety of participants in proceedings, their close relatives or spouse.[11]

In criminal proceedings e-justice systems such as audio-video recording of court hearings facilitate transparency. They are aimed at ensuring accuracy of court proceedings and establishing factual data in criminal trials. According to the Article 310 of the Criminal Procedural Code, audio-video

11 Criminal Procedural Code of the Kyrgyz Republic (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112308.

recording is mandatory only in criminal proceedings[12]. It provides access to information about criminal proceedings only for judges, court staff, prosecutors, and litigants.

The court provides copies of audio-video recording on CD to participants in proceedings at their request. Nevertheless, the right to obtain copies is limited. In the case of closed court hearings, the participants are not provided with audio-video recordings and summary minutes of the court session, though they are able to study them in the courthouse.[13]

In terms of the principle of openness of the courts, two e-justice systems provide access to court judgments: the "Digital Justice" e-portal and the publicly available website *act.sot.kg*. Nevertheless, the court must keep a balance between public access to court judgments and privacy of litigants and other participants in proceedings. In this regard, the Law of the Kyrgyz Republic "On Access to Information under the Jurisdiction of State Bodies and Local Self-Governance Bodies of the Kyrgyz Republic" with amendments adopted in 2016 establishes the obligation for the courts to depersonalize the personal data of litigants and other participants in the trial in published court judgments. Furthermore, it also determines limits for the disclosure of data privacy. For example, the following information cannot be disclosed by the court because it would allow participants in the trial (natural persons and legal entities) to be identified: (1) the name, patronymic, and surname of individuals; (2) the addresses of the place of residence or stay of citizens (natural persons), telephone numbers, or other means of communication such as email addresses; (3) passport data, personal numbers (codes), and information related to the civil status records of natural persons; (4) technical passport data of vehicles; (5) the name and identification number of a legal entity, legal claims against which have been recognized by the court as unlawful and unfounded; (6) any other information allowing the person to be identified.

However, disclosure of information is legal insofar as it concerns the surname and initials of the judge, court panel, prosecutor, defense counsel, officials of state and local self-government bodies, names, patronymics, surnames of citizens (natural persons) found guilty of committing crimes, and the name and identification number of a legal entity, claims against which are recognized by the court as legitimate and justified in the court

12 Ibid.
13 Ibid.

judgments. The publication of judicial acts involved in cases examined in closed trials is prohibited, except for requisite introductory and resolutive parts.[14]

In order to examine the impact of online publication of court judgments on the publicly available website *act.sot.kg*, 280 court judgments on domestic violence cases published by district and appellate courts in Bishkek, the capital city, and in regions between 2019 and 2021 were analyzed both in Kyrgyz and Russian. According to Article 75 of the Code on Misdemeanours, domestic violence was a misdemeanour entailing punishment in the form of a fine of the second category or correctional labour of the second category or public works of the second category.[15] In 2021 the Code on Misdemeanours became inoperative. After a dramatic increase in the number of cases of domestic violence during the Covid-19 pandemic, the Kyrgyz parliament returned the corpus delicti of domestic violence back to the Criminal Code adopted in 2021 (Maralbaeva and Pierobon 2023: 205-206). At present, domestic violence resulting in less serious harm to health is a crime embodied in Article 177 of the Criminal Code and punishable by corrective works for a term of 2 months to 1 year, or public works from 40 to 100 hours, or imprisonment for up to 5 years.[16]

Table 1. Data on when the court judgments in cases of domestic violence were issued.

Year	**Percentage of court judgments**
2019	25%
2020	63%
2021	12%

Source: Author's analysis of court judgments on domestic violence cases.

Among 280 court judgments on domestic violence cases that were examined within the framework of this research, the majority of cases (82%) were dismissed upon conciliation of perpetrators and victims of domestic

14 Law of the Kyrgyz Republic "On Access to Information under the Jurisdiction of State Bodies and Local Self-Governance Bodies of the Kyrgyz Republic" (2006). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/202010.

15 Code of the Kyrgyz Republic on Misdemeanors (out of legal force) (2019). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/111529.

16 Criminal Code of the Kyrgyz Republic (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112309.

violence. In a much smaller number of cases perpetrators were found guilty and convictions were issued (17.6%). Only in one case did the appellate court cancel the original judgment and return the case to the district court.

Table 2. The data on types of court judgments.

Type of court judgment	**Total amount**
Conviction	17.6%
Case dismissed	82%
Acquittal	0%
Court ruling that the original judgment be cancelled and the case returned to the district court	0.4%

Source: Author's analysis of court judgments in domestic violence cases.

The research revealed a mixed impact of online publication of court judgments on the principle of openness of courts and data protection taking the cases of domestic violence as an example. On the one hand, in a majority of court judgments personal data (such as the surnames and initials) of judges (67%), prosecutors (51%), and court session secretaries (59%), except defense counsels (15%) were disclosed in the court judgments. In a smaller number of court judgments on domestic violence cases these personal data were depersonalized. However, according to the Law "On Access to Information under the Jurisdiction of State Bodies and Local Self-Governance Bodies of the Kyrgyz Republic" this type of personal data should be disclosed because public officials and defense counsels, if they participated in the trial, fulfil the governmental function of administration of justice (Table 3).

Table 3. The personal data (i.e., surnames and initials) of judges, prosecutors, defense counsels, court session secretaries disclosed in the court judgments published online

Surname and initials	**Disclosed**	**Depersonalized**	**Did not participate in trial**
Judge	67%	33%	n/a
Prosecutor	51%	49%	n/a
Defense counsel	15%	29%	56%
Court session secretary	59%	41%	n/a

Source: Author's analysis of cases of domestic violence.

In the context of personal data of defendants, the study revealed that in all examined cases the surname, name, and patronymic of defendants were depersonalized and not disclosed. Only the initials of defendants were indicated in the court judgments. This complies with the provisions of the Law "On Access to Information under the Jurisdiction of State Bodies and Local Self-Governance Bodies of the Kyrgyz Republic."

However, other types of personal data such as defendants' date of birth, gender, family status, level of education, employment, prior criminal record, relationship between defendant and victim of the crime were disclosed in the majority of cases. Fewer cases depersonalized these types of personal data. The gender of defendants was not directly identified in the court judgment. It was determined according to the grammatical rules of the Russian and Kyrgyz languages (Table 4). Online publication of this data does not allow perpetrators to be identified. Based on the principle of the openness of the courts, anyone is allowed to participate in trials, except closed trials. In this case, the personal data of the perpetrator, victim, witnesses, and other third parties involved in the proceedings will be disclosed during the trials.

This issue raises the problem of the transformation of the concept of a public trial in the digital era. Previously, court judgments were not published online and only a small number of people attended court hearings. However, the online publication of court judgments dramatically changed the situation. Now the personal data disclosed in judgments are available online to the public not only in Kyrgyzstan but also abroad. In this regard, Winn has argued that "electronic records do not grow old, get moved to warehouses, or eventually get destroyed. They continue to exist, potentially forever" (Winn 2004: 317).

Table 4. The data of perpetrators disclosed in the court judgments published online

Type of data	Disclosed	Depersonalized
Date of birth	67%	33%
Gender	89%	11%
Family status	89%	11%
Level of education	91%	9%
Employment	79%	21%
Prior criminal record	77%	23%
Relationship between defendant and victim of the crime	83%	17%

Source: Author's analysis of cases of domestic violence conducted in December 2022.

The study revealed that in majority of cases of domestic violence men were perpetrators (84%). In a smaller number of cases women were perpetrators (5%). In 11% of cases the gender of the perpetrators was not disclosed (see Table 5).

Table 5. Gender of perpetrators in the cases of domestic violence

Gender	Amount
Male	84%
Female	5%
Not indicated	11%

Source: Author's analysis of cases of domestic violence conducted in December 2022.

In 75% of court judgments information on the dates of birth of victims of domestic violence was not disclosed, but in 25% of cases it was. In 98% of court judgments data on the employment of victims of domestic violence were not disclosed. Only in two cases they were disclosed. In 99.6% of cases data on the level of education of victims of domestic violence were not disclosed. The data were disclosed only in one case (0.4%). Online publication of these data does not allow the victims to be identified (see Table 6).

Table 6. The data on victims of domestic violence disclosed in the court judgments published online

Type of data	Disclosed	Not disclosed
Gender	89%	11%
Date of birth	25%	75%
Employment	2%	98%
Level of education	0.4%	99.6%

Source: Author's analysis of cases of domestic violence conducted in December 2022.

The study revealed that in the majority of cases (82%) women were the victims of domestic violence. In a much smaller number the victims were men (7%). The gender of victims of domestic violence was not indicated in the court judgments directly. It was determined on the basis of the rules of Russian grammar and the traditional peculiarities of the Kyrgyz language (see Table 7).

Table 7. Gender of victims of domestic violence

Gender	Amount
Female	82%
Male	7%
Not indicated	11%

Overall, the study revealed that, in the court judgments on domestic violence cases examined, district and appellate courts applied different approaches for the disclosure or depersonalization of the surnames and initials of judges, prosecutors, defense counsels, if they participated in the trial, and court session secretaries. For example, in a majority of the court judgments examined these types of personal data were disclosed. By contrast, in a smaller number of cases, these types of personal data were depersonalized, including the surnames and names of defense counsels. This shows that the courts do not adopt a single or consistent approach to the disclosure of the personal data of judges, prosecutors, defense counsels, if they participated in the trial, and court session secretaries, despite the fact that the Law "On Access to Information under the Jurisdiction of State Bodies and Local Self-Governance Bodies of the Kyrgyz Republic" establishes certain rules as mentioned previously. In addition, this case study also showed an equivocal impact of e-justice

systems on the principle of the openness of the courts. Online publication of court decisions on the publicly available website ensures the principle of openness of courts and provides access to court judgments for the public. However, published court judgment must not include any personal data of the victims of domestic violence.

Balancing Openness of the Courts and Data Protection in the Digital Era

The balance between the principle of openness of proceedings and data protection becomes one of the core issues in the context of the digital transformation of justice. In this regard, Winn has highlighted that "courts must balance the presumption of the openness of judicial proceedings against the need to keep certain types of information confidential – in particular, sensitive personal information" (Winn 2004: 311). According to the Law of the Kyrgyz Republic "On Personal Information" public access to sensitive personal information is prohibited, unless the subject of personal data gives his or her consent.[17]

In the context of the Kyrgyz Constitutional Court's judgments, balancing the principle of openness of proceedings and data privacy reveals jurisprudence addressing questions of privacy in other contexts. Winn has argued that "courts are accustomed to balancing the social benefits from the disclosure of personal information against the risk of harm that such disclosure may cause the individuals who are so identified"(Winn 2004: 312). For example, in the *Biometric Registration of Citizens Case*, the Constitutional Chamber of the Supreme Court determined that "the State, on the one hand, guarantees citizens the ability to control information about themselves and prohibits the disclosure of information of a purely personal nature, and, on the other hand, permits interference on legitimate grounds."[18]

Since online publication of court judgments on the official website *act.sot.kg* and the "Digital Justice" e-portal have provided public access to court judgments, the understanding of different treatment of paper court records and electronic court records should be recognized. Electronic court records cannot be treated in the same manner as paper ones. In this regard,

17 Law of the Kyrgyz Republic "On Personal Information" (2008). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/202269.

18 Reshenie Konstitutsionnoy Palatyi Verhovnogo Suda Kyirgyizskoy Respubliki po delu Toktokunova N. i Umetalievoi T. (2015). Available online at: https://constsot.kg/wp-content/uploads/2015/09/resh.-po-biomerii-1.pdf.

Winn has emphasized that "if the shift from paper to electronic court records takes place without appropriate safeguards, we will celebrate the abstract value of the free flow of judicial information at the cost of the privacy and security of litigants and other participants in the judicial system" (Winn 2004: 315). Moreover, "instead of increasing social respect for the judicial system, unrestricted access to court records will undermine the respect and confidence the courts … have traditionally enjoyed" (Ibid. 315)

Paper court records are protected under the concept of "practical obscurity" developed by the US federal courts. Practical obscurity means that "private information in public records is effectively protected from disclosure as the result of practical barriers to access. Practical barriers to access include travel to view the record, the passage of time, and the limits of indexing. When public records are accessible on the internet, those barriers are diminished."[19]

In the context of remote hearings via videoconferencing, the principle of the openness of the courts and the right to a public trial can be analyzed through the prism of the concept of practical obscurity. In July 2020, due to the Covid-19 pandemic, remote hearings via videoconferencing were rapidly implemented in all Kyrgyz courts in order to protect the health of judges, court staff, prosecutors, defense counsels, litigants, witnesses, and other third parties to the proceedings.[20]

A legal framework for remote hearings was established by the 2017 Criminal Procedural Code which allowed the interrogation of defendants, witnesses, and victims via videoconferencing. This legal provision helped to ensure access to criminal justice during the Covid-19 pandemic.[21]

In 2021 several amendments were introduced to criminal procedural legislation also due to the Covid-19 pandemic. In addition to remote hearings via videoconferencing, the 2021 Criminal Procedural Code established remote interrogations via videoconferencing of defendants (accused persons), victims, witnesses, experts and specialists (Articles 289, 290), as well as of

19 Practical obscurity. Available online at: https://dictionary.archivists.org/entry/practical-obscurity.html.

20 Decree of the Supreme Court of the Kyrgyz Republic "On Approval of the Regulations for Use of Videoconferencing in Courts of the Kyrgyz Republic" (2020). Available online at: http://admin-sot.sot.kg/public/sites/4/2020/10/Prikaz-138-ot-30.07.20g.-Ob-utverzhdenii-Reglamenta-ispolzovaniya-videokonferentssvyazi-v-sudah-KR.pdf.

21 Criminal Procedural Code of the Kyrgyz Republic (out of legal force) (2017). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/111530. The 2017 Criminal Procedural Code of the Kyrgyz Republic had legal force till 2021.

persons held in custody in a foreign state if such a procedure is allowed by an international treaty made by the Kyrgyz Republic that has entered into force (Article 516).[22]

Based on the data made available by the Judicial Department of the Supreme Court, 17,522 applications for remote hearings were submitted by judges via the "Remote Court Sessions" e-portal launched in June 2020.[23]

However, remote hearings via videoconferencing did not allow the public to join in online. People who wished to participate in proceedings could join in person in the courthouse. The courts did not share the online links for remote hearings. In the emergency situation created by the Covid-19 pandemic, the Supreme Court prioritized the protection of personal data of litigants, witnesses, and other third-party participants in criminal proceedings rather than the openness of the courts.

Since the restrictions caused by the Covid-19 pandemic were lifted, the number of remote hearings via videoconferencing has sharply decreased. Remote hearings have continued to be used for the interrogations of witnesses when they live far away from the court. (Interview with a court clerk conducted in June, 2022).

Cyber security and e-justice

The National Cyber Security Index (NCSI) is an evidence-based global index that measures the preparedness of countries to prevent cyber threats and manage cyber incidents. It is also a database with publicly available evidence materials and a tool for national cyber security capacity building.[24] NCSI is held and developed by the Estonian e-Governance Academy Foundation.[25]

The NCSI's remit includes cyber threats, analysis of legislation, established units, cooperation formats, and outcomes identification. Its indicators are based on the national cyber security framework. The major cyber threats include: (1) denial of e-services – services are made inaccessible; (2) data integrity breaches – unauthorized modifications; (3) data confidenti-

22 Criminal Procedural Code of the Kyrgyz Republic (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112308.
23 Audio-video recording of court hearings. Available online at: http://suddep.sot.kg/page/avf.
24 https://ncsi.ega.ee/methodology/.
25 https://ncsi.ega.ee/contact/.

ality breaches – secrets are exposed. The normal functioning of national information and communication systems and, through the ICT systems, electronic services (including critical e-services) can be affected by these threats. So, in order to respond to them, a state must have appropriate capacities for baseline cyber security, incident management, and general cyber security development.

The main measurable aspects of cyber security implemented by government include: (1) legislation in force – legal acts, regulations, orders, etc.; (2) established units – existing organizations, departments, etc.; (3) cooperation formats – committees, working groups, etc.;(4) outcomes – policies, exercises, technologies, websites, programs, etc. Country ratings are based on public evidence such as legal acts, official documents, and official websites.[26]

According to the NCSI 2023,[27] Kyrgyzstan obtained the second-highest score among countries in the Central Asian region, 37.66 out of 100. Kazakhstan had the highest score, 48.05. By contrast, Turkmenistan received 7.79 index points, the lowest score across the Central Asian region (see Table 8).

Table 8. National Cyber Security Index 2023.

Rank	Country	National Cyber security Index	Digital development
78	Kazakhstan	48.05	60.18
91	Kyrgyzstan	37.66	42.96
94	Uzbekistan	36.36	49.00
153	Tajikistan	10.39	34.56
164	Turkmenistan	7.79	No data

Source: National Cyber Security Unit, Version February 10, 2023[28]

Analysis of general cyber security indicators on the development of cyber security in Kyrgyzstan showed the data concerning three main aspects of the cyber security framework: general cyber security indicators, baseline cyber security indicators, and incident and crisis management. They revealed the achievements and gaps at the organizational, normative, and human resources levels.

26 https://ncsi.ega.ee/methodology/.
27 https://ncsi.ega.ee/compare/.
28 Ibid.

The *first group of indicators* comprises general cyber security indicators. They include cyber security development, cyber threats analysis and information, education and professional development in the field of cyber security, and contribution to global cyber security. In this context, Kyrgyzstan reveals medium to low scores in three indicators: cyber security policy development (71%), education and professional development (56%), and contribution to global cyber security (17%). There are no available data concerning cyber threat analysis and information (0%).

In terms of cyber security policy development, Kyrgyzstan recorded several achievements. The Coordinating Center for Ensuring Cyber Security of the State Committee for National Security of the Kyrgyz Republic is a specialized unit responsible for national cyber security policy development.[29] Under coordination by the Security Council, the State Committee for Information Technologies and Communications initiated the 2019–2023 Cyber Security Strategy and Action Plan made up of measures to implement the Strategy that were approved by a Decree of the Government of the Kyrgyz Republic in 2019.[30]

The 2019–2023 Cyber Security Strategy defines cyber security as "preserving the features of integrity (which may include authenticity and fault tolerance), availability and confidentiality of information of informational infrastructure objects, ensured through the use of a combination of means, strategies, security principles, security guarantees, risk management and insurance approaches, professional training, practical experience and technologies."[31]

Education and professional development are another partially successful examples within this group of indicators. Cyber safety competencies are taught in primary and secondary education curricula. There are also cyber security programs at the bachelor's and master's levels.

---

29 Decree of the Government of the Kyrgyz Republic "On Some Issues in the Sphere of Ensuring Cyber Security of the Kyrgyz Republic" (2020). Available online at: https://www.gov.kg/ru/npa/s/2498.

30 Strategy to Protect Cyber Space in Kyrgyzstan. Available online at: https://digital.gov.kg/ru/%d0%b4%d0%be%d0%ba%d1%83%d0%bc%d0%b5%d0%bd%d1%82%d1%8b/cyber/%d1%81%d1%82%d1%80%d0%b0%d1%82%d0%b5%d0%b3%d0%b8%d1%8f-%d0%b7%d0%b0%d1%89%d0%b8%d1%82%d1%8b-%d0%ba%d0%b8%d0%b1%d0%b5%d1%80%d0%bf%d1%80%d0%be%d1%81%d1%82%d0%b0%d0%bd%d1%81%d1%82%d0%b2%d0%b0-%d0%b2/.

31 Decree of the Government of the Kyrgyz Republic "On Approval of the Cyber Security Strategy of the Kyrgyz Republic for 2019-2023" (2019). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/15478?cl=ru-ru.

However, the country's contribution to global cyber security is not much developed. As a member-state of the Shanghai Cooperation Organization, Kyrgyzstan participates in *ensuring international information security*[32] (see Table 9).

Table 9. General Cyber Security Indicators: the case of Kyrgyzstan

Indicators	Score	Percentage
1. **Cyber security policy development**	**5 out of 7**	**71%**
1.1. Cyber security policy unit	**3**	
1.2. Cyber security policy coordination format	**0**	
1.3. Cyber security strategy	**1**	
1.4. Cyber security strategy implementation plan	**1**	
2. **Cyber threat analysis and information**	**0 out of 5**	**0%**
2.1. Cyber threats analysis unit	**0**	
2.2. Public cyber threat reports are published annually	**0**	
2.3. Cyber safety and security website	**0**	
3. **Education and Professional Development**	**5 out of 9**	**56%**
3.1. Cyber safety competencies in primary or secondary education curricula	**1**	
3.2. Bachelor's level cyber security program	**2**	
3.3. Master's level cyber security program	**2**	
3.4. PhD level cyber security program	**0**	
3.5. Cyber security professional association	**0**	
4. **Contribution to global cyber security**	**1 out of 6**	**17%**
4.1. Convention on Cybercrime	**0**	
4.2. Representation in international cooperation formats	**1**	
4.3. International cyber security organization hosted by the country	**0**	
4.4. Cyber security capacity building for other countries	**0**	

Source: National Cyber Security Unit, Version of February 10, 2023[33]

The second group of indicators are baseline cyber security indicators. They include protection of digital services, e-identification and trust services,

32 Shanghai Cooperation Organization. Available online at: https://ccdcoe.org/organisations/sco/.

33 https://ncsi.ega.ee/country/kg/.

protection of personal data. In this context, Kyrgyzstan achieves low, medium, and high scores in three out of four indicators: protection of digital services (20%), e-identification and trust services (78%), and protection of personal data (100%). There are no available data on protection of essential services (0%).

With respect to the protection of digital services, the Decree of the Government of the Kyrgyz Republic "On Approval of the Requirements for the Protection of Information Contained in the Databases of State Information Systems" establishes that public sector digital service providers must implement cyber security requirements and widely recognized security standards.[34]

In the context of e-identification and trust services, Kyrgyzstan has also recorded achievements as regards a unique persistent identifier and established requirements for cryptosystems. In addition, there is a legal framework for electronic identification and electronic signature. Both provide opportunities for digital interaction with state bodies and agencies via a public e-system "Tunduk."

Protection of personal data is the most successful example within this group of indicators. The Law of the Kyrgyz Republic "On Personal Information" was adopted in 2008 on the basis of international principles and norms in accordance with the Constitution and legislation of the Kyrgyz Republic. The purpose of this law was to ensure the protection of human and civil rights and freedoms related to the collection, processing, and use of personal data.[35] According to this law, a state body responsible for ensuring control over the compliance of personal data processing with the law's requirements and protection of the rights of personal data subjects was to be created. However, such a body came into being only in 2021. At present, the State Data Protection Agency under the Cabinet of Ministers of the Kyrgyz Republic fulfils these functions. The rapid development and implementation of ICT caused gaps in the Law of the Kyrgyz Republic "On Personal Information" which should be addressed in near future.

34 Decree of the Government of the Kyrgyz Republic "On Approval of Requirements for the Protection of Information Contained in the Databases of State Information Systems" (2017). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/11511.

35 State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic. Available online at: https://dpa.gov.kg/ru/about.

However, there are no available data on protection of essential services (Table 10).

Table 10. Baseline Cyber Security Indicators: the case of Kyrgyzstan

Indicators	**Score**	**Percentage**
Protection of digital services	1 out of 5	20%
Cyber security responsibility for digital services providers		
Cyber security standard for the public sector	1	
Competent supervisory authority	3	
Protection of essential services	0 out of 6	0%
Operators of essential services are identified	0	
Cyber security requirements for operators of essential services	0	
Competent supervisory authority	0	
Regular monitoring of security measures	0	
E-identification and trust services	7 out of 9	78%
Unique persistent identifier	1	
Requirements for cryptosystems	1	
Electronic identification	1	
Electronic signature	1	
Timestamping	0	
Electronic registered delivery service	0	
Competent supervisory authority	3	
Protection of personal data	4 out of 4	100%
Personal data protection legislation	1	
Personal data protection authority	3	

The third group of indicators is made up of incident and crisis management indicators, which include cyber incidents response, cyber crisis management, the fight against cybercrime, and military cyber operations. In this context, Kyrgyzstan shows medium and low achievement only in three out of four indicators: cyber incidents response (50%), cyber crisis manage-

ment (40%), fight against cybercrime (11%). There are no available data on military cyber operations (0%).

As far as the cyber incidents response unit is concerned, CERT-KG is part of the Coordination Center for Cyber Security of the State Committee of National Security of the Kyrgyz Republic.[36] CERT-KG counters cyber threats and regularly conducts technical checks and audits of the information systems of state bodies. For example, in 2019 67,000 samples of malicious software, 672,355 connections to malicious and potentially dangerous resources, and 8,534 attempts to redirect to malicious domains were registered. In addition, phishing emails targeting the public sector increased during the Covid-19 pandemic. Analysis of the enclosed malicious attachments provided by CERT-KG revealed that the file in question steals authentication credentials from various services from the computer. The cybercriminals used a trick word combination "qov.kg" instead of "gov.kg."[37] In addition, in 2021 the Internal Computer Incident Response Team of the Ministry of Digital Development was launched.

In the context of national-level cyber crisis management, the first national cyber drill exercise "Digital Kyrgyzstan 2021" was organized by the Coordination Center for Cyber security of the State Committee for National Security of the Kyrgyz Republic with the support of the OSCE Program Office in Bishkek and the International Telecommunication Union.[38]

The Chapter 40 "Cyber security crimes" of the Criminal Code of the Kyrgyz Republic (2021) establishes the *corpus delicti* of cybercrimes[39] (see Table 11).

36 https://ncsi.ega.ee/country/kg/.

37 Countering Cybercrime (2020). Available online at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CyberDrill-2020/CIS/%D0%9F%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F%20CERT-KG.pdf.

38 OSCE supports the first national cyberdrill in Kyrgyzstan (2021). Available online at: https://www.osce.org/programme-office-in-bishkek/484982.

39 Criminal Code of the Kyrgyz Republic (2021). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/112309.

Table 11. Incident and Crisis Management Indicators: the case of Kyrgyzstan

Indicators	**Score**	**Percentage**
Cyber incidents response	3 out of 6	50%
Cyber incidents response unit	3	
Reporting responsibility	0	
Single point of contact for international coordination	0	
Cyber crisis management	2 out of 5	
Cyber crisis management plan	0	40%
National-level cyber crisis management exercise	2	
Participation in international cyber crisis exercises	0	
Operational support of volunteers in cyber crisis	0	
Fight against cyber crime	1 out of 9	11%
Cybercrimes are criminalized	1	
Cyber unit	0	
Digital forensics unit	0	
24/7 contact point for international cybercrime	0	
Military cyber operation	0 out of 6	0%
12.1. Cyber operations unit	0	
12.2. Cyber operations exercise	0	
12.3. Participation in international cyber exercise	0	

Source: National Cyber Security Unit, Version of February 10, 2023[40]

The cyber security of the judicial system is an essential element for ensuring effective and successful e-justice implementation due to increasing cyber threats to the courts. It is aimed at preventing and responding to cyberattacks. The IT Agency "Adilet Sot" is responsible for ensuring the information security of the judicial system.

The courts hold sensitive personal data from judges, prosecutors, advocates, court clerks, litigants, and other third parties to proceedings. They operate databases of court judgments and other judicial acts, use e-case management systems, automated allocation of cases, audio-video record-

40 https://ncsi.ega.ee/country/kg/.

ings of proceedings, and carry out remote hearings via videoconferencing. These lead to increased data-governance responsibility.

Brian J. McLaughlin has argued that "there are multiple entry points for data breaches in the judicial branch ... judiciary case management systems, networks, servers, cloud storage, software programs, WiFi systems, employee devices, and an array of court-specific technology" (McLaughlin 2018: 68). Courts are public guardians of sensitive digital data assets. For instance, personal identifiers, victim information in domestic violence and sexual assault cases, confidential informants and search warrants in criminal cases, family court files involving children and families, testimony within sealed transcripts and recordings, medical and psychological reports, metadata within judiciary documents, employee personnel data in HR files, intellectual property and trade secrets, etc.

The 2018 Information Security of the Judicial System Concept is the main document which defines the approaches for ensuring comprehensive information security and establishes the procedure for the organization, the rules, and the distribution of functions and responsibilities for ensuring information security in the judicial system, as well as the information security requirements for the informational means used in the system.[41] It determines the threats to courts and the mechanisms for preventing and responding to them. In addition, the State Target Program "Development of the Justice System of the Kyrgyz Republic for 2023–2026" establishes obligations for judges and court staff to use an individual login and password, as well as an electronic digital signature. These are not allowed to be transferred to third parties.[42]

Overall, analysis of the 2018 Information Security of the Judicial System Concept revealed that it establishes only general provisions concerning cyber security for information resources in the judicial system such as AIS "Sud," automated allocation of cases, and AIS "Enforcement Proceedings." However, it does not include provisions to deal with the cyber security of court records of audio-video recordings of proceedings, remote hearings via videoconferencing, or the "Digital Justice" e-portal. These e-justice systems hold sensitive data assets that are recognized as objects of cyber security. For this reason, they should be included in the 2018 Concept. Likewise, the

41 The Information Security of the Judicial System Concept (2018). Available online at: http://suddep.sot.kg/post/informatsionnaya-bezopasnost-sudebnoj-sistemy-kr.

42 The State Target Program "Development of the Justice System of the Kyrgyz Republic for 2023-2026" (2023). Available online at: http://cbd.minjust.gov.kg/act/view/ru-ru/434916.

mechanism for ensuring the cyber security of these types of data should be determined in the Concept too.

In addition, two types of offences relating to information security are embodied in the Code of the Kyrgyz Republic on Offences. Article 228 establishes liability for unauthorized access to computer information, while Article 228 determines liability for the violation of requirements for protection of personal and commercial data. However, these articles entail fines in the sum of 20,000 KGS[43] to which only natural persons are liable, but not public officials. If these types of offences are committed by public officials, they would not be punishable under the Code of the Kyrgyz Republic on Offences. No liability leads to impunity. For this reason, these articles should be amended.

Conclusion

This chapter examines the impact of e-justice systems on the balance between the principle of the openness of courts and data protection, as well as on the cyber security of the judicial system in Kyrgyzstan. The research has revealed that online publication of court judgments has an equivocal impact on the principle of the openness of courts and data protection of litigants.

First, this issue raises the fundamental problem of the transformation of the concept of public trial perception in the digital era. In the predigital era, when few people attended court hearings, court judgments were not published online. In the digital era, court judgments published online are available for public viewing not only in Kyrgyzstan but also abroad. In this case the courts must depersonalize the personal data of litigants, victims, and other third-party participants in proceedings. Only the names, surnames, and patronymics (if any) of defendants found guilty of committing crimes can be disclosed in court judgments published online, according to national legislation.

Second, the different treatment of paper court records and electronic court records should be recognized at a national level. Electronic court records potentially can be stored forever on the Internet. For this reason, the court judgments published online must not include any personal data from victims, witnesses, and other third-party participants.

43 224 USD as of October 26, 2023.

Third, Kyrgyzstan has notched up several achievements in strengthening national cyber security. However, it has not yet fulfilled all the requirements for three main aspects of the cyber security framework: general cyber security indicators, baseline cyber security indicators, and incident and crisis management. There are some gaps on the organizational, normative, and human resources levels.

Fourth, e-justice systems hold sensitive data assets that are recognized as objects requiring cyber security. The 2018 Information Security of the Judicial System Concept should include provisions concerning the cyber security of court records of audio-video recordings of proceedings, remote hearings via videoconferencing, and use of the "Digital Justice" e-portal. In addition, the mechanism for ensuring the cyber security of these types of e-justice systems should be determined in the 2018 Concept.

Finally, the Code of the Kyrgyz Republic on Offences should be amended and entail the liability for unauthorized access to computer information and violation of requirements for protection of personal and commercial data of public officials responsible for storage and management of these types of data.

Acknowledgments

An early version of this chapter was presented at the International Legal Workshop "Strengthening the Rule of Law through E-justice" organized by Ala-Too International University in cooperation with Bielefeld University supported by the Volkswagen Foundation in October 2021 in Bishkek, Kyrgyzstan. This research was conducted in the framework of the postdoctoral fellowship program "Institutional Change and Social Practice. Research on the Political System, the Economy and Society in Central Asia and the Caucasus" funded by the Volkswagen Foundation. The author cordially thanks Prof. Dr. Andreas Vasilache (Project Director, Bielefeld University, Germany) for his support and guidance over the three years of the postdoctoral fellowship program, the editors of this book, Ms. Marie-Sophie Borchelt Camêlo and Dr. Aziz Elmuradov (Project Component Executives, Bielefeld University, Germany) for their valuable support and understanding, my tandem partner Dr. Chiara Pierobon (University of Washington, Seattle, USA) for her valuable recommendations concerning research methodology, Prof. Dr. Christoph Schuck (Project Director, TU Dortmund University, Germany) and Nora Becker (Project Component

Executive, TU Dortmund University, Germany) for organizing the international conference in Baku, Azerbaijan in September 2023, and all postdoctoral fellows for their kind cooperation.

References

Bodnár, Eszter (2016) "Transparency and openness of courts in the 21st Century. An issue worth researching on," *Iuris Dictio* 18, 153–164.

Faik, Isam, Thompson, Mark, and Walsham, Geoff (2019) "Designing for ICT-enabled openness in bureaucratic organizations: problematizing, shifting, and augmenting boundary work," *Journal of the Association for Information Systems* 20(6), 681–701.

Herrero, Alvaro and López, Gaspar (2010) *Access to Information and Transparency in the Judiciary*. Buenos Aires: Asociación por los Derechos Civiles. http://siteresources.worldbank.org/WBI/Resources/213798-1259011531325/6598384-1268250334206/Transparency_Judiciary.pdf>.

Maralbaeva, Aliia and Pierobon, Chiara (2023) "Ending Gender-Based Violence in Kyrgyzstan: Reflections on the Spotlight Initiative" In: Mihr, A., Sorbello, P. and Weiffen, B. (eds.) *Securitisation and Democracy in Eurasia*. Springer: Cham. https://doi.org/10.1007/978-3-031-16659-4_13, reproduced with permission of Springer Nature published under a CC-BY license http://creativecommons.org/licenses/by/4.0/, 201–215.

McLaughlin, Brian J. (2018) "Cybersecurity: protecting court data assets. *Trends in State Courts*, 67–72. https://ncsc.contentdm.oclc.org/digital/api/collection/tech/id/898/download.

Shergaziev, Chyngyz. (2023): Review of Digitalization in the Constitutional Court of the Kyrgyz Republic: Achievements and Plans, *Alatoo Academic Studies Journal*, Volume 1, 452–459.

UNDP (United Nations Development Programme) (2022) "E-justice: digital transformation to close the justice gap." https://www.undp.org/publications/e-justice-digital-transformation-close-justice-gap.

Winn, Peter A. (2004) "Symposium, online court records: balancing judicial accountability and privacy in an age of electronic information," *Washington Law Review*, 307–329. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/16.