ENCRYPTION IN KOSOVO

Protecting Civil Rights in the Digital Era

Aaron Spitler
2022 Early Career Fellowship Program
Internet Society

Disclaimer

This report was prepared for the Internet Society's 2022 Early Career Fellowship Program. The opinions expressed in this piece are the author's own and do not reflect the views of the Internet Society, Jožef Stefan Institute, and Open Data Kosovo. Written consent is required for the reproduction of this publication by any third party.

Acknowledgements

The author would like to thank the team at the Internet Society, namely Marilee D'Arceuil and Alejandra Prieto, for their assistance throughout the fellowship. They also appreciate the feedback provided by Tanja Pavleska and Samed Bajric at the Jožef Stefan Institute. Lastly, they are grateful for the support provided by Ariana Gjuli and their colleagues at Open Data Kosovo.

Contact Information

Aaron Spitler
Principal Author
2022 Early Career Fellow at the Internet Society
aaron.m.spitler@gmail.com

Table of Contents

I. General Overview

Encryption tools have been viewed as a means of guaranteeing the fundamental rights of connected citizens. However, in the case of Kosovo, those shaping policy have not maximized the potential of these technologies. This report brings attention to this critical issue, outlining how stakeholders across all sectors can take action to protect the freedoms of citizens. The paper begins by outlining how cryptographic techniques have been used to defend civil liberties while also contextualizing them in the Balkan country. The following segments are devoted to unpacking relevant Kosovar law, comparing these existing measures to the European Union (EU)'s General Data Protection Regulation (GDPR). A supplemental table offers details on these key statutes, highlighting specific areas where policy measures could be better aligned with EU standards. Finally, the report ends with a set of recommendations that major actors could consider to uphold the rights of Kosovars in our digital age.

II. Topic Background

Encryption, a process in which data is encoded to limit its availability, has been used to uphold the rights of individuals across the globe. These safeguards help ensure that information passed between users is not compromised, providing peace of mind to citizens worried about the activities of businesses and governments. Not only have these tools been used to shield the right to privacy, they are also considered an "enabler" for liberties like the freedom of expression.[1] Considering its utility in securing the confidentiality of communications, attempts to undercut the technology should be viewed with suspicion. Countless organizations involved with human rights have strongly come out in favor of these technical measures, calling for full transparency when government officials seek to bypass these cryptographic controls.[2] Ultimately, encryption will prove useful to individuals at a moment where all aspects of life are undergoing a process of digitization.

---

[1] *Encryption: A Matter of Human Rights*, Amnesty International (2016), https://www.amnestyusa.org/reports/encryption-a-matter-of-human-rights/.

[2] *Human rights and encryption*, United Nations Educational, Scientific and Cultural Organization (2016), https://unesdoc.unesco.org/ark:/48223/pf0000246527?1=null&queryId=e05fdd78-68b9-4ff3-b7ce-b998b0c0cf01.

In Kosovo, a country located in the heart of Southeastern Europe, awareness of the benefits provided by these technologies is limited. Experts have argued that while citizens are "connected," users may not recognize the myriad threats to their data found outside and within the country. Kosovar law, for instance, allows state institutions to freely intercept citizen communications without following due process.[3] Outdated regulatory frameworks, coupled with minimal public education, create a dismal scenario in which fundamental rights are left unprotected by technical safeguards. Policymakers unfamiliar with encryption may be willing to cast aside the technology without question, citing the need to assure the security of the public at large.[4] Average citizens, in turn, suffer significant consequences. Without highlighting the value of encryption in the debate on rights, stakeholders in Kosovo will lose out on a resource that is invaluable at a time defined by technological upheaval.

[3] "My Password! My Privacy! My My, The Digital Age!", Kosovo 2.0 (2016), https://kosovotwopointzero.com/en/password-privacy-digital-age/.
[4] "Kosovo Surveillance Build-up Raises Privacy Concerns", Balkan Insight (2021), https://balkaninsight.com/2021/12/31/kosovo-surveillance-build-up-raises-privacy-concerns/.

III. Existing Legislation

A number of statutes and policies related to the protection of data have been implemented over the years. The Constitution of Kosovo stipulates that access to information generated by individuals must be regulated by legislation. The Law on Personal Data Protection (No. 06/L-082), LPPD, was designed to address those obligations, providing instruction on how institutions can effectively safeguard the privacy of users irrespective of their background.[5] Beyond outlining the responsibilities of the state, it also makes note of specific measures that can be deployed to accomplish this task. "Technical and logical-technical procedures," which include encryption technologies, were explicitly referenced as potential protections that could be used by future officials.[6] From looking at these documents, it is reasonable to assume that preserving civil liberties was top-of-mind for policymakers in Kosovo. Encryption, as a result, has long been seen as a means to this end.

---

[5] *Kosovo – Data Protection Overview*, OneTrust Data Guidance (2022), https://www.dataguidance.com/notes/kosovo-data-protection-overview.

[6] *Data Protection Laws of the World – Kosovo*, DLA Piper (2021), https://www.dlapiperdataprotection.com/index.html?t=law&c=XK#:~:text=The%20competent%20national%20data%20protection,order%20to%20protect%20the%20rights.

However, measures that call for leveraging this technology have not always been put into practice. For instance, while the LPPD is mindful of citizens' needs, there are mechanisms by which the government can refute their petitions. In fact, officials can refuse requests to cease the processing of information if they can offer a rationale, granting institutions the latitude to infringe upon freedoms protected by encryption.[7] Glaring vulnerabilities in policy solutions are one reason why cryptographic technologies have been largely underutilized. Experts have highlighted how a lack of knowledge is at fault. Older officials may not understand privacy issues, whereas younger policymakers might not fully take advantage of encryption-enabled technologies.[8] Across the board, citizens in Kosovo remain under-informed about these protections, as well as how policies designed to safeguard their freedoms online may fail them. Awareness, therefore, is needed sooner rather than later.

---

[7] *Kosovo – Data Protection 2019*, Global Legal Group (2019), https://www2.deloitte.com/content/dam/Deloitte/al/Documents/legal/DP19_Chapter-27_Kosovo.pdf.

[8] *Cybersecurity Capacity Review – Republic of Kosovo*, Global Cyber Security Capacity Centre (2020), https://gcscc.ox.ac.uk/files/cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf.

IV. GDPR Statutes

By and large, the debate on the value of encryption in Kosovo has been shaped by developments in the European Union. Policymakers in Pristina have modeled their solutions on the General Data Protection Regulation (GDPR), a slate of reforms passed in 2016 related to the protection of data. This legislation places the onus of protecting the rights of individuals onto groups who have access to data.[9] It seeks to provide users with a degree of autonomy, wresting control over their data away from actors whose intentions may be seen as questionable. In emphasizing the need for accountability, the GDPR helps ensure that actors would no longer be able to manipulate data generated by individuals without facing consequences.[10] Nearly six years since its passage, the regulation remains the "gold standard" for policy that strives to protect the interests of citizens amid overreach from governments and businesses alike.

[9] "What is GDPR? The summary guide to GDPR compliance in the UK", Wired (2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[10] "Everything you need to know about GDPR", The Verge (2018), https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice.

The GDPR also outlines how to bolster protections for rights. Specifically, it calls for the adoption of "technical measures" by organizations working with data, a line which policymakers interpret to mean tools like encryption. Leveraging cryptographic technologies would generally minimize the amount of personal data processed by relevant actors.[11] In practice, the technique would restrict how information could be used by entities, reducing the risk of misuse and exploitation. Experts have argued that, over time, the legislation would trigger a shift in which actors would become comfortable with these controls on their access to data. Mainstreaming "encryption by design" would benefit users of all walks of life, giving them a sense of security that was not present in the past.[12] This aspect of the GDPR has forced many stakeholders to consider how they are meeting the needs of users who rely on their products and services.

[11] "WTF is GDPR?", TechCrunch (2018), https://techcrunch.com/2018/01/20/wtf-is-gdpr/?guccounter=1.
[12] "GDPR: Ground zero for a more trusted, secure internet", The Conversation (2018), https://theconversation.com/gdpr-ground-zero-for-a-more-trusted-secure-internet-95951.

V. Comparison Chart

Law Name	Basic Description	Key Encryption-Related Provisions	Relevant GDPR Sections
Law on Protection of Personal Data (No. 06/L-082)[13] - Passed 2019	Determines the rights and responsibilities of organizations with respect to the protection of data generated by individuals	Article 5 ("Lawful processing of personal data") stipulates that processing data for reasons that do not relate to why it was collected must use safeguards like encryption Article 31 ("Safety of processing") calls for the pseudonymization and encryption of data as a means of mitigating the risk of manipulation Article 34 ("Communication of a personal data breach to the data subject") absolves those who control data of responsibility for breaches if they implemented safeguards like encryption	Article 6 ("Lawfulness of processing") clarifies that the processing of data for purposes outside the reasons it was collected must include safeguards like encryption Article 32 ("Security of processing") mandates that processors must use safeguards like encryption when working with data Article 34 ("Communication of a personal data breach to the data subject") states that those who control data are not liable for breaches if they used safeguards like encryption
Law on Protection of Whistleblowers (No. 06/L-085)[14] -	Outlines how to protect whistleblowers	Article 7 ("Rights of whistleblower") outlines how	Article 5 ('Principles relating to processing of personal data") outlines

[13] https://assembly-kosova.org/Uploads/Data/Documents/Lawno06L-082_NBuSkkM44v.pdf

[14] https://md.rks-gov.net/desk/inc/media/701773B8-903F-476F-9D1E-2F7CC2C86A84.pdf

Passed 2018	and their information in both the public and private sectors	whistleblowers are the confidentiality of the information they disclosed Article 12 ("Protection of personal data of whistleblowers") mandates that the handling of whistleblower data must be done in accordance with laws on data protection Article 20 ("Public whistleblowing") maintains that a whistleblower is obliged to respect laws relating to the protection of personal data	how safeguards should be in place to secure data Article 25 ("Data protection by design") underscores how those in control of information are obliged to implement safeguards that preserve privacy Article 28 ("Processor") sets the expectation that processors use the appropriate safeguards, including encryption, when handling data
Law on General Administrative Procedure (No. 05/L-031)[15] - Passed 2016	Establishes expectations for the conduct of individuals working in the public sector, including how to hand personal information	Article 4 ("Principle of lawfulness") states that organs of the government must provide services in a manner that respects the rights of all persons Article 9 ("Principle of open administration") mandates that public authorities bear responsibility for protecting the personal data of Kosovar citizens	Article 6 ("Lawfulness of processing") requires that any service rendered by the government which involves the data of individuals must not infringe upon their rights Article 24 ("Responsibility of the controller") raises that those in control of data must implement technical measures which may include

[15] http://www.mei-ks.net/repository/docs/annex_9_law_on_general_administrative_procedure.pdf

		Article 92 ("Right of the party to inspect the files and receive information") raises that releasing information depends on whether the materials contain any personal information	encryption technologies Article 86 ("Processing and public access to official documents") charges that agencies responsible for the provisions of services must respect the right to protection of data when performing tasks related to administration
Law on Interception of Electronic Communications (No. 05/L-030)[16] - Passed 2015	Explains the conditions by which the state can intercept the communications of individuals in Kosovo	Article 27 ("Retention and destruction of data within the interception facility of the Chief State Prosecutor - CSP") mandates that any data intercepted by authorities must remain with the CSP if it is relevant to an ongoing investigation Article 28 ("Retention and destruction of data within the Kosovo Police interception facility") charges that any data intercepted by authorities must remain with the Kosovo Police if it is relevant to an ongoing investigation Article 34 ("Functions of the Commissioner") highlights how the	Article 5 ("Principles relating to processing of personal data") outlines how the analysis of data must be done for legitimate purposes while also adopting technical safeguards Article 10 ("Processing of personal data relating to criminal convictions and offences") raises that the processing of data related to criminal cases must also adopt appropriate safeguards Article 32 ("Security of processing") states that all actors processing data must use safeguards in all cases

[16] http://old.kuvendikosoves.org/common/docs/ligjet/05-L-030%20a.pdf

		Commissioner for Oversight of the Electronic Communications Interception Procedure must coordinate with the National Agency for the Protection of Personal Data to ensure data privacy and security	
Law on Information Society Government Bodies (No. 04/L-145)[17] - Passed 2013	Delineates how responsibilities for the administration of e-services will be divided amongst agencies	Article 6 ("Functions of the Agency) charges that the Agency for Information Society is responsible for protecting the data of individuals Article 7 ("General Director of the Agency") charges how the agency head must provide professional advice to government agencies on all aspects related to the information society Article 8 ("Structure, the relevant official and coordination in ICT") states that all institutions must have a department that manages issues related to information	Article 5 ("Principles relating to the processing of personal data") outlines the obligations of actors who process data, including the safeguards they chose to adopt Article 24 ("Responsibility of the controller") explains that those who have access to data must work within their organizations to ensure that processing is safe and secure Article 32 ("Security of processing") states that all processors of data must abide by the same protocols and practices

17 http://old.kuvendikosoves.org/common/docs/ligjet/Law%20on%20information%20society%20government%20bodies.pdf

		technologies	
Law on Police (No. 04/L-076)[18] - Passed 2012	Provides authorization for the Police of the Republic of Kosovo, as well as clarifying how they use citizen's data in their criminal investigations	Article 5 ("Relationship between the Police and the Ministry") outlines how the Minister of Internal Affairs has the right to collect, maintain, and analyze collected data Article 31 ("Collection, Retention, Processing, Analysis, Use and Deletion of Data") charges that the Kosovo Police are responsible for protecting individual data Article 55 ("Issuance of sub legal acts") outlines how the General Director of the Kosovo Police is responsible for the proper management of personal data	Article 24 ("Responsibility of the controller") states that actors with access to data must adopt appropriate safeguards when working with collected data Article 26 ("Joint controllers") states that in scenarios where two or more actors have control of the data, they are required to detail how they intend to abide by the law Article 37 ("Designation of the data protection officer) mandates that an official be responsible for the processing of data within an organization

[18] https://www.kosovopolice.com/wp-content/uploads/2021/03/LAW-No.-04-L-076-ON-POLICE_2-March-2012.pdf

Law on Electronic Communication (No. 04/L-109)[19] - Passed 2012	Underscores how private information should be managed in laws related to virtual communications	Article 9 (“Regulatory Objectives”) outlines how the Regulatory Authority of Electronic and Postal Communications is responsible for protecting the integrity of personal data Article 65 (“Transparency and Publication of Information”) charges that providers should inform subscribers that they have the right to remove their data from any directories published by the outlet Article 85 (“Security, Integrity and Reliability”) highlights how entrepreneurs supporting public communications networks are encouraged to adopt appropriate technical safeguards	Article 21 (“Right to object”) focuses on how individuals have the right to prevent actors from handling their data in a manner they deem inappropriate Article 24 (“Responsibility of the controller”) mandates that actors in charge of data take precautions when processing this information Article 32 (“Security of processing”) outlines how actors must adopt technical safeguards when engaging in data analysis
Law on Civil Status	Regulates how the status of inhabitants is decided, including how officials manage	Article 4 (“Data Personal Character”) explains that information collected by the Civil Status Registry is personal in	Article 9 (“Processing of special categories of personal data”) describes how data deemed personal in nature are require

[19] http://old.kuvendikosoves.org/common/docs/ligjet/109%20Law%20on%20Electronic%20Communications.pdf

(No. 04/L-003)[20] - Passed 2011	data generated by these individuals	character, requiring certain protections Article 6 ("Collection and civil status data exchange with third parties") requires that data collected by the government on status be protected Article 7 ("Rights Protections") highlights how protections must be in place to safeguard the information of citizens in Kosovo	certain protections Article 24 ("Responsibility of the controller") underscores how actors in charge of data must adopt safeguards for processing Article 32 ("Security of processing") emphasizes the need for protections like encryption when handling the data of individuals
Law on Access to Public Documents (No. 03/L-215)[21] - Passed 2010	Clarifies how public institutions can release official documents, including those which feature personal data	Article 12 ("Exceptions from the right of access to documents") underscores how information collected by the government can be withheld in situations where it infringes upon the right to privacy Article 17 ("The Ombudsperson Institution") places responsibility for the release of information, as well as its security, onto The Ombudsperson Institution	Article 7 ("Conditions for consent") requires that an individual be informed on how their data will be handled, including any protections adopted by the actor responsible for processing Article 24 ("Responsibility of the controller") sets the parameters for how controllers of information should conduct their business, especially regarding the protections for data Article 37 ("Designation of the data protection

[20] http://old.kuvendikosoves.org/common/docs/ligjet/Law%20on%20civil%20status.pdf
[21] https://www.rti-rating.org/wp-content/uploads/Kosovo.pdf

		Article 23 (“Protection of personal data”) outlines that public institutions must secure the explicit consent of Kosovar citizens before releasing their personal data	officer”) emphasizes how an official should be responsible for how information is protected in entities that handle data
Law on Prevention and Fight of the Cyber Crime (No. 03/L-166)[22] - Passed 2010	Shares how government officials can combat criminal activity in the digital domain while respecting civil rights	Article 5 (“Prevention, security and information campaigns”) states that actors involved in cybersecurity conduct activities focused on the prevention of cybercrime Article 10 (“Unauthorized interception”) explains that the interceptions of data, including communications, is an offense punishable by law Article 26 (“Legal provisions for providing information and data, necessary for the foreign authorities”) outlines how law enforcement in Kosovo should cooperate with foreign authorities in criminal investigations that involve the	Article 24 (“Responsibility of the controller”) raises that actors managing data take “organizational measures,” which could include cooperation with partners on the promotion of encryption Article 34 (“Communication of a personal data breach to the data subject”) outlines how actors responsible for data should take action to notify subjects whose information has been compromised Article 44 (“General principles of transfer”) requires that Kosovo ensure that the protection of data remains firm when sending information to entities outside its borders

[22] http://old.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf

		misuse of personal data	

Figure 1.0 - General overview of Kosovar legislation related to data privacy and encryption protections

VI. Initial Observations

From the outset, it is clear that measures put forward by policymakers were designed to be mindful of protections when handling data. Several pieces of legislation, such as 2012's Law on Electronic Communication, make it clear that agencies of the government are responsible for preserving the integrity of this information. However, when it comes to the measures that should be implemented to achieve this goal, many statutes are vague in their suggestions. Some policies, including the Law on Protection of Personal Data passed in 2019, make mention of tools like encryption. Yet others only go so far as expecting that entities "protect" the information that they have gathered from citizens throughout the country. Choosing to minimize, if not ignore, the benefits provided through encryption may ultimately serve to undermine the privacy of citizens. Critically, this oversight may facilitate the erosion of fundamental rights like the freedoms of speech and expression.

This legislative framework also outlines the government agencies which uphold data privacy. For instance, 2015's Law on the Interception of Personal Communications identifies the National Agency for the Protection of Personal Data (NAPPD) as the main entity whose mandate relates to digital rights. However, 2013's Law on Information Society Government Bodies grants authority to the Agency for Information Society (AIS), while 2012's Law on Police highlights the obligations of the Kosovo Police. In short, the variety of actors whose work involves the protection of data may be problematic. Changes in governments, and ministries, over the years is likely to have affected coordination among organizations. Turnover might have also led officials to redefine the mandates of entities, increasing the risk of confusion and miscommunication for those responsible for cybersecurity. As a result, decision-makers do a disservice to citizens, which may also have the effect of eroding their confidence in the government.

VII. Policy Recommendations

Stakeholders in Kosovo must pay more attention to incorporating encryption into legislation related to the protection of data. There are a

number of ways that these actors can address these gaps in policy. A list of these options, broken down by decision-maker, can be seen below:

Government Ministries

Policy Solutions

1. *Conduct internal review of relevant legislation to clarify how encryption technologies are a standard practice for data protection*

2. *Launch mapping exercise to identify key institutions with open access to personal information and define their core obligations to ensuring data protection*

3. *Equip existing institutions, such as the NAPPD and AIS, with enforcement, monitoring, and evaluation mechanisms to assist Kosovar citizens whose personal data may have been manipulated by external actors*

Relevant Actors

- *AIS*
- *NAPPD*
- *Ministry of Education, Science, Technology and Innovation (MESTI)*

International Partners

Policy Solutions

1. *Strengthen bilateral cooperation between EU entities, including the European Union Agency for Cybersecurity (ENISA), and Kosovar*

institutions, especially the NAPPD, to ensure greater policy harmonization

2. *Lobby government agencies to implement transparency measures that may assuage citizen concerns about data exploitation*

3. *Convene multi-party dialogues which bring together government leaders and citizen groups to discuss how digital rights can inform the direction of Kosovo's cybersecurity strategy*

Relevant Actors

- *ENISA*
- *European Union Office in Kosovo (EU in Kosovo)*
- *Council of Europe Office in Pristina (COE in Kosovo)*

Business Community

Policy Solutions

1. *Collaborate with government officials to educate principle decision-makers on the general value of encryption technologies for cybersecurity matters*

2. *Participate in regional events focused on encryption technologies to gather valuable information on its diverse applications from international firms*

3. *Coordinate with major stakeholders in civil society and the public sector to create a whole-of-society approach to defending digital rights*

Relevant Actors

- *Kosovo Association of Information and Communication Technology (STIKK)*
- *Innovation Centre Kosovo (ICK)*
- *American Chamber of Commerce in Kosovo (AmCham Kosovo)*

Civil Society Organizations

Policy Solutions

1. *Provide logistical support to citizen groups who aim to reduce the risk of data misuse by external actors*

2. *Create public forums where citizen groups can share their individual concerns about data manipulation*

3. *Consult government officials on how to center digital rights when crafting cybersecurity policy*

Relevant Actors

- *Open Data Kosovo (ODK)*
- *Next Gen Networks Institute (NGN)*
- *Institute for Free Market Economics (IFME)*

VIII. Key Conclusions

Cybersecurity, including the manipulation of data, is a priority for policymakers in Pristina. Over the years, a framework has been

constructed to ensure that threats in cyberspace are addressed. Yet this arrangement has not always centered the needs of citizens. Critically, the lack of awareness on encryption sends a message to Kosovars that their data may not always be secure. Shortcomings in policy will not only provide “gaps” that could be exploited by actors unconcerned with the priorities of citizens. They will also offer an “opening” in which actors, including the government, can accumulate masses of information that infringe upon other freedoms enjoyed by Kosovars. These issues were magnified by the pandemic, in which individuals throughout the country were forced to spend their time online. Ultimately, they will only grow in importance as more aspects of life become “digitized,” increasing the opportunities actors will have to exploit the user data.

Considering the stakes, action must be taken to fortify the protections available to citizens in Kosovo. The recommendations listed above provide a roadmap that stakeholders from all sectors could follow as they look to the future. Leaders in government could eliminate vagaries in legislation while also clarifying how agencies can remain compliant with laws relating to privacy. Meanwhile, partners found abroad could leverage their influence to increase the degree of collaboration between citizens

and their government, creating an opportunity for breakthroughs that may not exist otherwise. Finally, groups in civil society are well-positioned to place pressure on actors in government and business for violations they commit. Taken together, these reforms can create an environment where the use of encryption becomes more commonplace. Above all, they can make a difference in guaranteeing that freedoms like speech and expression in the digital space are not disregarded by those with influence in Kosovo.