

*Gordana Lažetić**
*Boban Misoski***
*Suat Shaqirov****

PREREQUISITES FOR RATIFICATION OF THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CYBERCRIME CONVENTION

Summary

The Budapest Convention remains the most significant international treaty on cybercrime and electronic evidence. North Macedonia ratified the Convention in 2004 and the First Additional Protocol in 2005. The Second Additional Protocol introduces mechanisms for direct cooperation with service providers, expedited MLA, and JITs, focusing on subscriber data, domain name registration information and traffic data. Only Serbia, Hungary, and Costa Rica have ratified it so far. For North Macedonia, ratification requires legislative reforms (Criminal Procedure Code, Law on Electronic Communications, Law on International Cooperation in Criminal Matters), institutional reforms (specialized units, training, video conferencing), and policy alignment with GDPR-equivalent standards. Public awareness initiatives are also essential to build trust and legitimacy. Ratification is not just a formal act but a systemic transformation: it strengthens international cooperation, enhances protection of victims in cyberspace, and ensures justice in the digital age.

Keywords: Budapest Cybercrime Convention, Additional Protocol, Direct cooperation, Mutual Legal Assistance (MLA), Joint Investigations

I. INTRODUCTION

The Council of Europe Convention on Cybercrime (the Budapest Cybercrime Convention),¹ was opened for signatures in 2001 and entered into force in 2004. Since the June 2026, total of 82 countries are parties to the Convention, including all EU Member States and with more than 30 European States.² The Council of Europe began to work on criminal justice responses to cybercrime from the mid-1980s onwards.

North Macedonia had ratified the Budapest Cybercrime Convention on 15.09.2004, and the First Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems on 14.11.2005.³ It was the first international treaty to

* Gordana Lažetić, PhD., Professor, Ss. Cyril and Methodius University in Skopje, Iustinianus Primus Faculty of Law, email: gordana2206@gmail.com, g.lazetic@pf.ukim.edu.mk, ORCID - <https://orcid.org/0000-0002-0719-3293>

** Boban Misoski, PhD., Professor, Ss. Cyril and Methodius University in Skopje, Iustinianus Primus Faculty of Law email: b.misoski@pf.ukim.edu.mk ORCID - [Boban Misoski \(0009-0008-4843-7857\)](https://orcid.org/0009-0008-4843-7857) - [My ORCID](#)

*** Suat Shaqirov, Ph.D. student, Ss. Cyril and Methodius University in Skopje, Iustinianus Primus Faculty of Law, email: suatshaqiri2016@gmail.com

¹ Convention on Cybercrime, (ETS No. 185), Budapest, 23.XI.2001, <https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf>

² <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>

³ Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), <https://www.coe.int/en/web/cybercrime/first-additional-protocol>; <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189>

focus explicitly on cybercrime and electronic evidence and even after 25 years since its entrance into force, while still remains the most significant international treaty in the area.⁴

First Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems from 2003 complemented the Budapest Cybercrime Convention regarding Xenophobia and Racism committed via computers. The first additional Protocol extends the list of offences to provide for the criminalization of the dissemination of racist and xenophobic material through computer systems; racist and xenophobic motivated threat and insult, and the denial, gross minimization, approval or justification of genocide or crime against humanity.⁵ Regarding the Second Additional Protocol to the Budapest Convention,⁶ in 2012 the Cybercrime Convention Committee (T-CY) created a working group to consider the issues. Eventually a working group transformed into the Cloud Evidence Group. The Cloud evidence group explores solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance.⁷ In 2021 the Cybercrime Convention Committee concluded work on the Second Additional Protocol to the Convention. Guidance Notes adopted by the Committee explain how the Convention can be applied to address new challenges. The Second Additional Protocol to the Budapest Convention (CETS No. 224) facilitates cross-border access to electronic evidence. It entered into force on September 1, 2024, after reaching the required five ratifications. As of mid-2026, only two Council of Europe member states have fully ratified the Protocol: Serbia (2023) and Hungary (2026), and also non-member state of Costa Rica (2026).⁸

This new Protocol is to provide for more effective cooperation on cybercrime and electronic evidence between public authorities but also with private sector entities across borders. Electronic evidence is crucial not only for investigating cybercrime but any type of crime. The Protocol is needed to protect individuals and their rights against crime and for victims to obtain justice.⁹ The ratification of this Protocol will enhance the international cooperation and protection of victims in cyberspace.¹⁰

In the light of the proliferation of cybercrime and other offences involving electronic evidence, and in the context of technological change and uncertainty regarding jurisdiction, additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations.¹¹

During the past decade the European Commission has been taken steps to strengthen EU cooperation in the fight against terrorism, organised crime and cybercrime. It recognizes that cyber

⁴ Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence, 27.07.2022, <https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access>

⁵ Protocol on xenophobia and racism, <https://rm.coe.int/2021-bc20-factsheets-p1/1680a47c06>

⁶ The Second Additional Protocol to the Budapest Convention (CETS No. 224)

⁷ Cloud Evidence Group, <https://www.coe.int/en/web/cybercrime/ceg>

⁸ <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224>

⁹ Protocol on enhanced co-operation and disclosure of electronic evidence, <https://rm.coe.int/2021-bc20-factsheets-p2/1680a47c07>

¹⁰ Filippo Spiezia, International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime, ERA Forum 23(1), April 2022, DOI: [10.1007/s12027-022-00707-8](https://www.researchgate.net/publication/359726177), <https://www.researchgate.net/publication/359726177> International cooperation and protection of victims in cyberspace welcoming Protocol II to the Budapest Convention on Cybercrime

¹¹ Criminal justice access to data in the cloud: challenges, France T-CY (2015)10 Provisional Cybercrime Convention Committee (T-CY), Discussion paper prepared by the T-CY Cloud Evidence Group, 26 May 2015 Strasbourg, <https://rm.coe.int/1680304b59>

criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information. This is very significant when taking into account the technological developments especially the cloud computing, so challenging issue is gathering electronic evidence in real time from other jurisdictions and ensuring its admissibility in court.¹²

In North Macedonia there is awareness for the need of preparations for the ratification of the Second Additional Protocol to the Budapest Convention, by clarification of the legal steps towards ratification and highlighted key challenges and opportunities. All those issues are important for understanding the benefits of ratification and how it can strengthen Macedonian criminal justice response to cybercrime.¹³

II. PREREQUISITES FOR RATIFICATION OF THE SECOND PROTOCOL

Ratifying the Second Additional Protocol to the Budapest Convention requires domestic legislation updates, explicit human rights safeguards, and formal declarations, with EU member states specifically mandated to invoke joint investigation teams, data protection limits, and notification mechanisms under Articles 7 and 14. There is a need for legislative and policy reforms before ratification, namely, domestic legislation must be enacted or amended to empower authorities to comply with the protocol's core mandates.

1. Direct Cooperation with Providers

Regarding direct cooperation with providers it is important for the legal authority to permit domestic and foreign competent authorities to directly request Domain Name Registration Information (DNRI) and Subscriber Information from foreign service providers or registrars without strictly relying on traditional Mutual Legal Assistance (MLA) channels.

Domestic law must explicitly authorize competent authorities to directly request Domain Name Registration Information (DNRI) and Subscriber Information from foreign service providers or registrars. Traditionally, such requests relied on MLA channels, which are slow and bureaucratic. The protocol envisions a streamlined process where investigators can bypass MLA for basic subscriber data, provided safeguards are in place. This reform requires amendments to criminal procedure codes and telecommunications laws to recognize foreign service providers as legitimate recipients of lawful requests.

2. Mutual Legal Assistance issues

Mechanisms that facilitate expedited MLA requests for subscriber information and traffic data, as well as immediate cooperation in emergencies are significant issues. Namely, the Second Additional Protocol emphasizes expedited MLA procedures for subscriber information, traffic data, and emergencies. National legislation must establish mechanisms for urgent cooperation, including deadlines for response, simplified formats, and electronic transmission of requests. This ensures that time-sensitive investigations—such as cyberattacks or imminent threats—are not delayed by lengthy diplomatic channels. Reforms may include creating specialized MLA units, digital portals, and statutory obligations for authorities to prioritize urgent requests.

¹² The EU Agenda on Security, https://ec.europa.eu/commission/presscorner/detail/en/ip_15_4865

¹³ <https://www.coe.int/en/web/cybercrime/-/cybersee-north-macedonia-advances-preparations-for-the-ratification-of-the-second-additional-protocol-to-the-convention-on-cybercrime>

3. Joint Investigations and Modern Tools

Domestic law must provide a legal basis for joint investigation teams (JITs) with foreign counterparts. This includes recognition of shared jurisdiction, rules for evidence collection, and safeguards for defendants' rights. Additionally, legislation should permit the use of video conferencing for witness testimony, suspect interviews, and coordination meetings. These reforms align national practice with the protocol's cooperative spirit, enabling authorities to work seamlessly across borders while respecting due process.

III. KEY PREREQUISITES FOR RATIFICATION

Significant prerequisite for ratification is when states adopt a personal data protection framework that satisfies Chapter V of the Protocol, ensuring adequate safeguards for the cross-border transfer of personal data.¹⁴ Chapter V provides a binding human rights framework to ensure data protection when cross-border electronic evidence is shared, emphasizing purpose limitation, data minimization, and individual redress. Namely, any cross-border transfer of personal data ensures an "adequate level of protection," meaning that the receiving jurisdiction must provide safeguards equivalent to those guaranteed under the Protocol. This requirement is not merely technical but grounded in Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life. The European Court of Human Rights (ECtHR) has consistently held that inadequate data protection can constitute a violation of this right.

The most prominent case directly handling this issue is *Big Brother Watch and Others v. the United Kingdom* (2021).¹⁵ The core of the case is intelligence sharing and data transfers. While commercial cross-border data transfers (like EU-to-US corporate flows) are famously handled by the Court of Justice of the European Union (CJEU), the ECtHR rules on state accountability under the ECHR. CJEU in cases *Schrems I* and *Schrems II* as landmark legal cases, decided that invalidated EU-US data transfer deals, specifically *Safe Harbor* and the *Privacy Shield*. They ruled that these frameworks failed to protect EU citizens from broad U.S. government surveillance.

In *Big Brother Watch*, human rights organizations challenged the UK's bulk interception programs (uncovered by Edward Snowden), which included receiving mass data from foreign intelligence agencies (such as the US National Security Agency). In this landmark judgment, the Grand Chamber of the ECtHR ruled that the UK government's bulk interception of communications powers "did not contain sufficient 'end-to-end' safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse", thus violating the rights to privacy and freedom of expression.¹⁶

The notion of "adequacy" is central. It requires states to assess whether the third country has legally binding safeguards, independent supervisory authorities, and effective remedies for individuals. This mirrors the EU General Data Protection Regulation (GDPR), Article 45, which sets out similar adequacy requirements for international transfers. The GDPR prohibits transfers

¹⁴ Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention, European Digital Rights (EDR), <https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf>

¹⁵ Case of *Big Brother Watch and others v. The United Kingdom*, (*Applications nos. 58170/13, 62322/14 and 24960/15*), Judgment 25.05.2021

¹⁶ UK: Europe's top court rules UK mass surveillance regime violated human rights, May 2021, <https://www.amnesty.org/en/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/>

of personal data to countries without an adequacy decision unless additional safeguards (standard contractual clauses, binding corporate rules) are in place.

Amendments are required in domestic law to allow competent authorities to give effect to foreign orders (e.g., expedited production of subscriber information).¹⁷ A state must formally designate authorities to receive and act upon cross-border requests, including the points of contact for emergency mutual assistance.¹⁸

Upon ratification, Parties are required to make specific declarations—such as whether they will require mutual legal assistance channels to process requests for subscriber information before direct provider requests.¹⁹

IV. ROADMAP FOR LEGISLATIVE, INSTITUTIONAL AND POLICY REFORMS

When analyzing the Additional Protocol, in order to implement its provisions into the national legal system and by this to adopt the Protocol it is important to mention that there is a need for integrated approach both in legislative, institutional and policy aspects. Hence, we will closely elaborate these reform activities that are influenced by the Additional Protocol divided into three phases.

1. Legislative Reforms

The legislative amendments shall be the first phase so that the legislation have to be aligned with innovative cross-border mechanisms since the Second Protocol transforms international cyber-investigations by allowing direct cross-border requests to private entities, bypassing traditional, slow Mutual Legal Assistance (MLA) channels for non-content data. The Second Protocol focuses on three types of non-content data: (1) domain name registration information (DNRI); (2) subscriber information and (3) traffic data.²⁰

The first phase shall be focused toward alignment of the following three laws: Criminal Procedure Code, Law on electronic communication and Law on International Cooperation in Criminal Matters

Criminal Procedure Code shall be amended to be in alignment with Articles 6 and 7 of the Protocol. Harmonization with article 6 shall be provided if there is explicitly authorized domestic law enforcement to issue orders directly to domain registries or registrars located in a foreign State Party to disclose Domain Name Registration Information (DNRI).²¹ When analyzing execution mechanics from article 7, there is a need to grant domestic prosecutors the statutory power to issue

¹⁷ Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data, <https://www.eurojust.europa.eu/sites/default/files/assets/files/article-8-of-the-second-additional-protocol-to-the-convention-on-cybercrime-giving-effect-to-orders-from-another-party-for-expedited-production-of-subscriber-information-and-traffic-data.pdf>

¹⁸ Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency, <https://www.eurojust.europa.eu/publication/article-9-second-additional-protocol-convention-cybercrime-expedited-disclosure-stored>

¹⁹ Second Protocol on enhanced cooperation and disclosure of electronic evidence, <https://rm.coe.int/t-cy-28-item-8-second-rotocol-v1/1680abddfd>

²⁰ Defined as set out in Articles 1 and 18, paragraph 4 of the Budapest Convention

²¹ Davies, G., Kennedy-Mayo, D., The promise and pitfalls of the Second Protocol to the Budapest Convention: Assessing its impact on EU and UK cross-border criminal investigations, *New Journal of European Criminal Law*, Vol. 17(1), 2026, pp. 101–123, <https://doi.org/10.1177/20322844261419413>

a standardized "Production Order" directly to a foreign Service Provider (SP) in another State Party. This order can mandate the disclosure of subscriber information (identity, contact details, payment logs) under the service provider's control.

Law on Electronic Communications need to be adjusted to the Second Protocol, as well. There is a need to introduce obligations for providers to respond to lawful requests from foreign authorities, with safeguards for privacy and data protection. An important provision of the Second Protocol aimed at facilitating cooperation between the Parties and private entities is Article 8. Article 8 provides a legal basis for a requesting Party to issue an order to be submitted as part of a request to another Party and for the requested Party to have the ability to give effect to that order by compelling a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control.²² Article 8 introduces a clear statutory obligation for local ISPs and telecommunication companies to comply when a foreign authority submits a certified out-of-country order. The local provider must be legally empowered and compelled to produce subscriber information or traffic data within their possession.²³

When taking into account the article 14 of the Protocol, there is a need for adjustment of the Law on electronic communication so that data disclosed to a foreign authority may only be used for the specific investigation or judicial proceeding listed in the order. There is a need for the local providers to notify the domestic Data Protection Authority (DPA) if a cross-border data transfer suffers a security breach. Providers must securely maintain logs of all incoming foreign requests and subsequent disclosures for a minimum period (e.g., 3 years) to allow for independent DPA audits.

The Law on international Cooperation in Criminal Matters need to be amended with the aim of expedited MLA procedures for subscriber and traffic data, including emergency cooperation clauses in accordance with the articles 9 and 10 of the Protocol. Expedited traffic data rules are important for adjustment of the legislation with the article 9 of the Protocol. Namely, traffic data requires a higher standard of protection than subscriber data. The amendment must allow a fast-tracked path where domestic authorities can request a foreign state to compel its local provider to release traffic data quickly, provided a judicial warrant is attached. There is also need to establish an emergency "fast-track" framework, so if there is an immediate threat to life or a risk of critical infrastructure failure, domestic law enforcement can bypass all formalities. It encompasses possibilities for direct emergency request, meaning to provide an opportunity for sending an emergency request straight to a foreign service provider for immediate voluntary disclosure of subscriber/traffic data. This is a reason why there is a necessity for the 24/7 network backstop, so if the provider cannot or will not comply, the amendment must authorize the domestic 24/7 cybercrime contact point to immediately utilize the official Budapest Convention 24/7

²² Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Explanatory Report, Cybercrime Convention Committee (T-CY), [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%220900001680a48e4b%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%220900001680a48e4b%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}), paras 124-126

²³ Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving Effect to Orders from Another Party for Expedited Production of Subscriber Information and Traffic Data, EUROJUST, September 2024, <https://www.eurojust.europa.eu/sites/default/files/assets/files/article-8-of-the-second-additional-protocol-to-the-convention-on-cybercrime-giving-effect-to-orders-from-another-party-for-expedited-production-of-subscriber-information-and-traffic-data.pdf>

network to route an urgent emergency assistance request to the foreign central authority for immediate execution.²⁴

2. Institutional Reforms

Second phase shall be focused toward institutional aspects as support of the legislative changes and alignments.²⁵ Amendments of the Law on International Cooperation in Criminal Matters toward expedited MLA mechanisms shall be support by establishing specialized units within the Ministry of Justice and Public Prosecutor's Office to handle urgent requests electronically, with strict deadlines. Since, there is an ARO Office within the PPO, there is a need to strengthen its capacities and provide necessary resources so that it can contribute toward more efficient way of taking actions.²⁶

Practical experience and trainings regarding participation in the Joint Investigation Teams (JITs) shall be also in the focus of interest. The procedures and conditions governing the operation of joint investigation teams, such as their specific purposes; composition; functions; duration and any extension periods; location; organisation; terms of gathering, transmitting and using information or evidence; terms of confidentiality; and terms for the involvement of the participating authorities in investigative activities taking place in another country's territory, shall be as agreed between competent authorities of the involved countries.²⁷

In the Republic of North Macedonia, there is already such an opportunity for participation in JITs in the Law on International Cooperation in Criminal Matters. However, there is a need to strengthen the capacities of prosecutors for successful participation in JITs, understanding their establishment, meaning, role, manner of proceeding, international cooperation as well as including recognition of shared jurisdiction and evidence admissibility.

Providing conditions for video conferencing is also important. The central authorities of the requested and requesting Parties shall communicate directly regarding organizing video conferencing.²⁸ Legislative amendments shall permit remote testimony, suspect interviews, and cross-border coordination and there shall be guidelines or rules for preforming successful video conferencing with all necessary conditions.

3. Policy and capacity building

The ratification of the Second Additional Protocol to the Budapest Convention requires states to adopt clear and coherent policy frameworks that balance investigative powers with fundamental rights. Aligning reforms with GDPR-equivalent standards is not only a technical requirement but a matter of policy credibility. By embedding privacy safeguards into national legislation, governments demonstrate their commitment to rule of law and human rights, while ensuring that new investigative tools are used responsibly.

Policy reforms must be matched with capacity building across the justice chain. Judges, prosecutors, and law enforcement need specialized training to handle digital evidence, cross-border requests, and new cooperation mechanisms introduced by the Protocol. Capacity building ensures that institutions can operationalize policy commitments, reducing the gap between law on

²⁴ Workshop 9 – International cooperation on cybercrime and electronic evidence: the Second Protocol to the Budapest Convention on Cybercrime, November 2025, <https://www.coe.int/en/web/cybercrime/workshop-9-international-cooperation-on-cybercrime-and-electronic-evidence-the-second-protocol-to-the-budapest-convention-on-cybercrime>

²⁵ Davies, G. & Kennedy-Mayo, D., op.cit.

²⁶ Закон за канцеларија за поврат на имот, Службен весник на РСМ, бр. 66/2024

²⁷ In accordance with the article 12 of the Second Amendment.

²⁸ In accordance with the article 11 of the Second Amendment

paper and law in practice. Continuous professional development also strengthens resilience against evolving cyber threats and enhances international cooperation.

Public awareness initiatives connect policy and capacity building by fostering legitimacy and trust. Informing service providers, civil society, and citizens about new procedures ensures transparency and accountability, while motivating victims and witnesses to engage with institutions. This nexus between policy and capacity highlights that reforms are not merely legal adjustments but systemic transformations. Effective ratification of the Protocol thus depends on integrated strategies that combine strong policy design, institutional capacity building, and public engagement.

V. GOOD PRACTICES IN FOREIGN LEGAL FRAMEWORKS AS A GUIDANCE FOR MACEDONIAN LEGAL REFORM

When analyzing good practices in legislative amendments in different European countries it is worth mentioning legal framework about direct cooperation with providers. This aligns with article 7 of the Second Additional Protocol, which provides a legal basis for cross-border requests to service providers, while at the same time is expected to be implement into the Macedonian legal system.

In this line it is notable to mention **France's** experience where there were amendments to the Code of Criminal Procedure to allow prosecutors to directly request subscriber information from foreign service providers, bypassing traditional MLA channels. Amendments to Article 230-34 with Article 230-34-1 and Article 706-96-1 with Article 706-96-2 in the French Penal Procedural Code creates an amendment allowing the collection of evidence through audio and visual recordings, as well as geolocation data, by accessing technological devices. This is particularly relevant in cases related to terrorism and organized crime. Additionally, new paragraphs have been amended to Articles 230-36 and 706-97 of the French Penal Procedural Code. As a result of these amendments, investigation authorities are for the first time in a penal procedural code, empowered to secretly obtain evidence from electronic devices through remote activation. In this context, the current article will address how and which authorities can listen to a person during an investigation, the offenses that allow this measure to be applied, the limitations of cataloged offenses, and how eavesdropping for intelligence purposes will be conducted.²⁹

Serbia, on the other hand, was the first country in the world to ratify the Second Additional Protocol to the Budapest Convention (February 2023). To achieve this, Serbia undertook legislative steps to align its Criminal Procedure Code, laws on electronic communications, and MLA framework with the Protocol's requirements, ensuring direct cooperation with providers, expedited MLA, and joint investigations.³⁰

During the ratification process on 9 February 2023, Serbia deposited its instrument of ratification at the Council of Europe, becoming the first state to do so, but prior to ratification, Serbia reviewed its criminal justice legislation to ensure compatibility with the Protocol's

²⁹ Balci, Murat & Kerim Çakir. "Investigation Authorities' Ability to Secretly Obtain Evidence from Electronic Devices Through Remote Activation in The French Penal Procedural Code". *Bilişim Hukuku Dergisi*, 5.2 (2023): 126-150.

³⁰ <https://www.coe.int/en/web/cybercrime/-/serbia-becomes-first-state-to-ratify-the-second-additional-protocol-to-the-convention-on-cybercrime>

enhanced cooperation tools. There was a law enacted in 2022 regarding the ratification of the Protocol, as well.³¹

CyberSEE supports Serbia's efforts to implement the Second Additional Protocol to the Convention on Cybercrime.³² Criminal Procedure Code have been amended so to allow direct requests for subscriber information and domain name registration data from foreign service providers, bypassing traditional MLA channels. There was also legal basis established for Serbia's participation in Joint Investigation Teams (JITs) and use of video conferencing for witness testimony and investigative coordination. Law on International Legal Assistance introduced expedited MLA procedures, including electronic transmission of requests and statutory deadlines for urgent cooperation. Law on Electronic Communications was amended to recognize lawful requests from foreign authorities and ensure providers comply with disclosure obligations, while embedding privacy safeguards. Aside legislative changes, Serbia considered establishing a working group to guide legislative reform and oversee implementation of the Protocol. So, as an EU candidate country, Serbia aligned reforms with EU Council Decision 2023/436, ensuring consistency with EU member state practices.

Hence, **North Macedonia** should follow the Serbia's steps while preparing for ratification of the Protocol. There is a need for synchronizing the criminal procedure, MLA framework, and electronic communications law with the Protocol's mandates, while simultaneously building institutional capacity and private sector partnerships. These reforms will ensure compliance, strengthen cybercrime investigations, and prepare the country for effective ratification and implementation of the Second Additional Protocol. Before North Macedonia ratifies the Second Additional Protocol to the Budapest Convention, it must amend several core laws and establish organizational structures to ensure compliance. Legislative reforms should focus on enabling direct cooperation with providers, expedited MLA procedures, and joint investigations, while organizational reforms should strengthen coordination among justice institutions and the private sector

Criminal Procedure Code shall be amended with provisions to allow prosecutors and investigators to directly request Domain Name Registration Information (DNRI) and Subscriber Information from foreign service providers, bypassing traditional MLA channels. Law on International Cooperation in Criminal Matters shall introduce expedited MLA procedures, including electronic transmission of requests, statutory deadlines for urgent cooperation, and emergency clauses. Law on Electronic Communications shall be updated to impose obligations on domestic providers to respond to lawful requests from foreign authorities, with privacy safeguards. Regarding the Data Protection Alignment, reforms shall comply with EU GDPR-equivalent standards, balancing investigative needs with privacy rights.

When organizational steps are analyzed, the Serbia example shall be followed – establishing a multi-stakeholder body – working group (Ministry of Justice, Interior, Prosecutor's Office, judiciary, telecom regulators, Internet Service Providers, banks) to oversee legislative drafting and implementation. In the same time there is a need for capacity building, new curriculums and trainings of judges, prosecutors, and law enforcement on handling electronic evidence, expedited MLA, and cross-border cooperation. There is also a need for formalizing

³¹ Zakon o potvrđivanju Drugog dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu o pojačanoj saradnji i otkrivanju elektronskih dokaza, ("Sl. glasnik RS - Međunarodni ugovori", br. 7/2022), http://demo.paragraf.rs/demo/combined/Old/t/2022_12/MU_007_2022_006.htm

³² <https://www.coe.int/en/web/cybercrime/-/cybersee-supports-serbia-s-efforts-to-implement-the-second-additional-protocol-to-the-convention-on-cybercrime>

cooperation with ISPs, telecoms, and financial institutions to ensure readiness for direct requests and emergency disclosures. The last but not at least, efforts toward raising awareness and transparency and inform civil society and service providers about new procedures to build trust and ensure accountability.

VI. CONCLUSION

The Second Additional Protocol to the Council of Europe Budapest Convention on enhanced cooperation and disclosure of electronic evidence aims to enhance cooperation among the Parties, as well as between the Parties and service providers and other entities, for obtaining disclosure of electronic evidence for the purpose of criminal investigations or proceedings. The ratification of the Second Additional Protocol to the Budapest Convention represents a decisive step in strengthening North Macedonia's criminal justice response to cybercrime. The Protocol provides innovative mechanisms for direct cooperation with service providers, expedited mutual legal assistance, and joint investigations, all of which are essential in an era where electronic evidence is central to nearly every type of crime. By adopting these reforms, North Macedonia would not only align itself with international standards but also enhance its ability to protect victims and uphold justice in cyberspace.

A critical prerequisite for ratification lies in legislative reforms. Amendments to the Criminal Procedure Code, the Law on Electronic Communications, and the Law on International Cooperation in Criminal Matters are necessary to empower prosecutors and investigators to directly request subscriber and domain name registration information, streamline MLA procedures, and enable participation in joint investigation teams. These legislative changes will ensure that Macedonian authorities can act swiftly and effectively, while embedding safeguards for privacy and human rights.

Equally important are institutional reforms. Specialized units within the Ministry of Justice and the Public Prosecutor's Office must be established to handle urgent requests electronically, supported by training programs that build capacity among judges, prosecutors, and law enforcement. Strengthening the ability to participate in joint investigation teams and enabling video conferencing for cross-border testimony will ensure that Macedonian institutions are prepared to operationalize the Protocol's cooperative spirit. Institutional readiness is the bridge between legislative commitments and practical enforcement. Ratification requires a coherent policy and capacity building framework. Aligning reforms with GDPR-equivalent standards demonstrates credibility and respect for fundamental rights, while public awareness initiatives foster legitimacy and trust among service providers, civil society, and citizens. By combining strong policy design, institutional capacity building, and transparent communication, North Macedonia can ensure that ratification is not merely a formal act but a systemic transformation. This integrated approach will prepare the country to meet the challenges of cybercrime, strengthen international cooperation, and guarantee justice in the digital age.

Bibliography:

1. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), <https://www.coe.int/en/web/cybercrime/first-additional-protocol:https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=189>

2. Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data, <https://www.eurojust.europa.eu/sites/default/files/assets/files/article-8-of-the-second-additional-protocol-to-the-convention-on-cybercrime-giving-effect-to-orders-from-another-party-for-expedited-production-of-subscriber-information-and-traffic-data.pdf>
3. Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency, <https://www.eurojust.europa.eu/publication/article-9-second-additional-protocol-convention-cybercrime-expedited-disclosure-stored>
4. Balci, Murat & Kerim Çakir. "Investigation Authorities' Ability to Secretly Obtain Evidence from Electronic Devices Through Remote Activation in The French Penal Procedural Code". *Bilişim Hukuku Dergisi*, 5.2 (2023): 126-150.
5. Case of Big Brother Watch and others v. The United Kingdom, (*Applications nos. 58170/13, 62322/14 and 24960/15*), Judgment 25.05.2021
6. Convention on Cybercrime, (ETS No. 185), Budapest, 23.XI.2001, <https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf>
7. Criminal justice access to data in the cloud: challenges, France T-CY (2015)10 Provisional Cybercrime Convention Committee (T-CY), Discussion paper prepared by the T-CY Cloud Evidence Group, 26 May 2015 Strasbourg, <https://rm.coe.int/1680304b59>
8. Cloud Evidence Group, <https://www.coe.int/en/web/cybercrime/ceg>
9. Davies, G., Kennedy-Mayo, D., The promise and pitfalls of the Second Protocol to the Budapest Convention: Assessing its impact on EU and UK cross-border criminal investigations, *New Journal of European Criminal Law*, Vol. 17(1), 2026, pp. 101–123, <https://doi.org/10.1177/20322844261419413>
10. Protocol on enhanced co-operation and disclosure of electronic evidence, <https://rm.coe.int/2021-bc20-factsheets-p2/1680a47c07>
11. Protocol on xenophobia and racism, <https://rm.coe.int/2021-bc20-factsheets-p1/1680a47c06>
12. Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention, European Digital Rights (EDR), <https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf>
13. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Explanatory Report, Cybercrime Convention Committee (T-CY), [https://search.coe.int/cm#{%22CoEIdentifier%22:\[%220900001680a48e4b%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680a48e4b%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}), paras 124-126
14. Second Protocol on enhanced cooperation and disclosure of electronic evidence, <https://rm.coe.int/t-cy-28-item-8-second-rotocol-v1/1680abddfd>
15. Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence, 27.07.2022, <https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access>
16. Spiezia, Filippo, International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime, *ERA Forum* 23(1), April 2022, DOI: [10.1007/s12027-022-00707-8](https://www.researchgate.net/publication/359726177), <https://www.researchgate.net/publication/359726177>
[International cooperation and protection of victims in cyberspace welcoming Protocol II to the Budapest Convention on Cybercrime](https://www.researchgate.net/publication/359726177)
17. The Second Additional Protocol to the Budapest Convention (CETS No. 224)

18. The EU Agenda on Security,
https://ec.europa.eu/commission/presscorner/detail/en/ip_15_4865
19. UK: Europe's top court rules UK mass surveillance regime violated human rights, May 2021, <https://www.amnesty.org/en/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/>
20. Workshop 9 – International cooperation on cybercrime and electronic evidence: the Second Protocol to the Budapest Convention on Cybercrime, November 2025, <https://www.coe.int/en/web/cybercrime/workshop-9-international-cooperation-on-cybercrime-and-electronic-evidence-the-second-protocol-to-the-budapest-convention-on-cybercrime>
21. Закон за kancelarija za povrat na imot, Služben vesnik na РСМ, бр. 66/2024
22. Zakon o potvrđivanju Drugog dodatnog protokola uz Konvenciju o visokotehnoškom kriminalu o pojačanoj saradnji i otkrivanju elektronskih dokaza, ("Sl. glasnik RS - Međunarodni ugovori", br. 7/2022), http://demo.paragraf.rs/demo/combined/Old/t/t2022_12/MU_007_2022_006.htm
23. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=185>
24. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=224>
25. <https://www.coe.int/en/web/cybercrime/-/cybersee-north-macedonia-advances-preparations-for-the-ratification-of-the-second-additional-protocol-to-the-convention-on-cybercrime>
26. <https://www.coe.int/en/web/cybercrime/-/serbia-becomes-first-state-to-ratify-the-second-additional-protocol-to-the-convention-on-cybercrime>
27. <https://www.coe.int/en/web/cybercrime/-/cybersee-supports-serbia-s-efforts-to-implement-the-second-additional-protocol-to-the-convention-on-cybercrime>