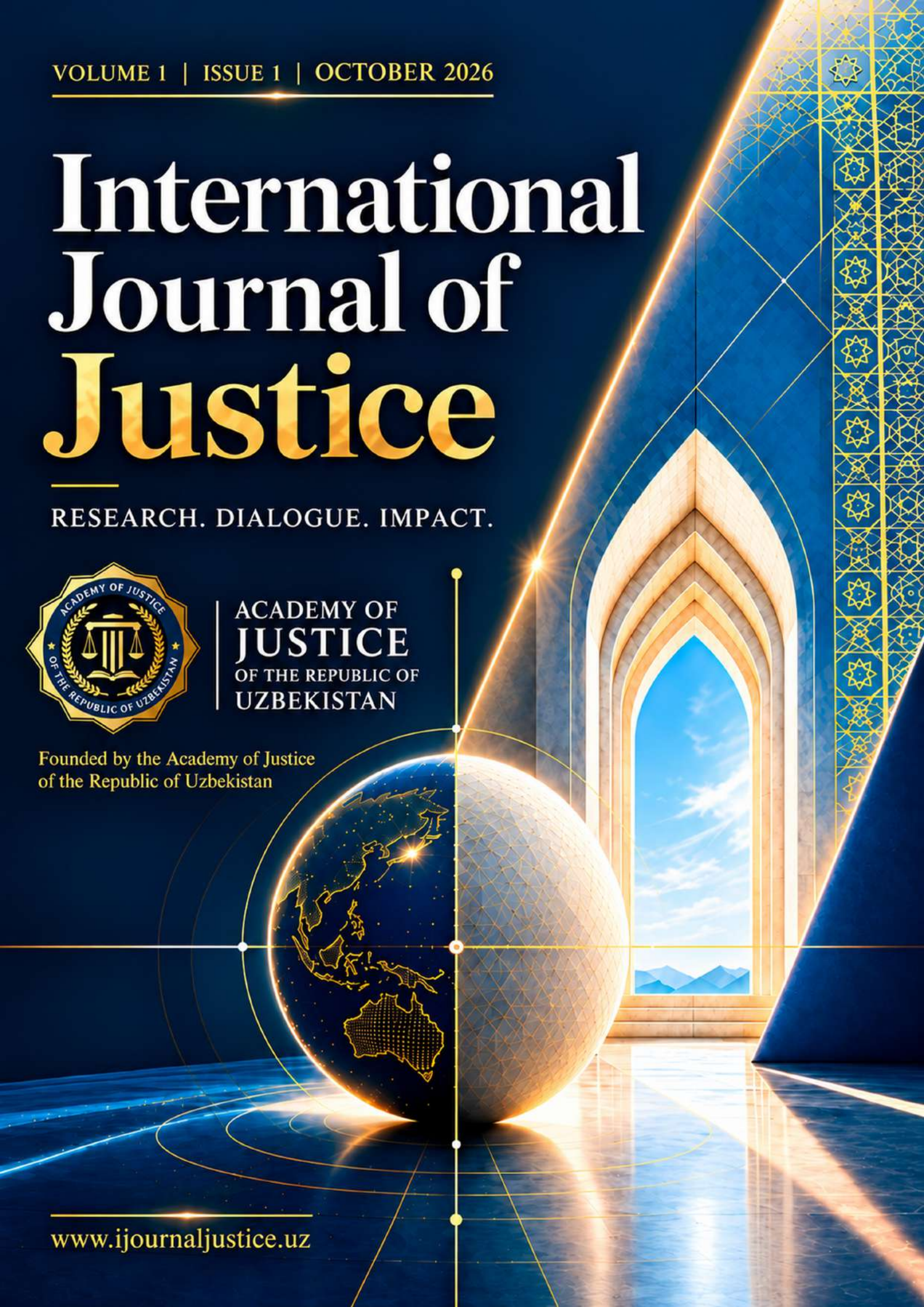
VOLUME 1 | ISSUE 1 | OCTOBER 2026

International Journal of Justice

RESEARCH. DIALOGUE. IMPACT.

ACADEMY OF JUSTICE OF THE REPUBLIC OF UZBEKISTAN

Founded by the Academy of Justice of the Republic of Uzbekistan



www.ijournaljustice.uz

EDITORIAL BOARD

International Journal of Justice



EDITOR-IN-CHIEF

Sherzod Yoqubjonovich Abduqodirov

Rector of the Academy of Justice of the Republic of Uzbekistan

Doctor of Sciences in Law (DSc), Associate Professor



DEPUTY EDITOR-IN-CHIEF

Nodirbek Saparbaevich Salaev

Vice-Rector of the Academy of Justice of the Republic of Uzbekistan

Doctor of Sciences in Law (DSc), Professor

MEMBERS OF THE EDITORIAL BOARD



Anselmo Reyes

Doctor of Philosophy (PhD) in Law, Professor

Judge of the Singapore International Commercial Court



Dilshod Urinbaevich Aripov

Doctor of Sciences in Law (DSc), Professor

Vice-Rector of the Academy of Justice of the Republic of Uzbekistan



Akrom Ikromovich Toshpulatov

Doctor of Sciences in Law (DSc), Professor

Director of the Parliamentary Research Institute under the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan



Shakhriyor Bakhtiyorovich Bakaev

Doctor of Philosophy (PhD) in Law

Responsible Official of the Administration of the President of the Republic of Uzbekistan



Borzu Sabahi

Doctor of Sciences in Law (DSc), Professor

International Arbitrator



Dilshod Shavkatovich Israilov

Doctor of Philosophy (PhD), Associate Professor

Head Specialist of the Department for Coordination of Research Activities of the Academy of Justice of the Republic of Uzbekistan



Yesemurat Sultamuratovich Kanyazov

Candidate of Legal Sciences in Law (PhD)

Director of the Institute for Retraining and Advanced Training of Legal Personnel under the Ministry of Justice of the Republic of Uzbekistan



Yevgeniy Vyacheslavovich Kolenko

Doctor of Philosophy (PhD), Professor

First Deputy Head of the Law Enforcement Academy of the Republic of Uzbekistan



Krisztina Karsai
Doctor of Sciences in Law (DSc), Professor
Head of the Institute of Criminal Law and Criminal Sciences at the University of Szeged



Lorenzo Mateo Bujosa Vadell
Doctor of Philosophy (PhD) in Law, Professor
Professor at the University of Salamanca



Maged Mamdouh Kamel Shebaita
Doctor of Philosophy (PhD), Professor
International Arbitrator, Doctoral Candidate at the University of London



Ivan Georgievich Nikonov
Doctor of Philosophy (PhD) in Law
Responsible Official of the Administration of the President of the Republic of Uzbekistan



Malikakhon Pirnazarovna Kalandarova
Doctor of Philosophy (PhD), Associate Professor
Deputy Chairperson of the Supreme Court of the Republic of Uzbekistan



Islambek Rustambekovich Rustambekov
Doctor of Sciences in Law (DSc), Professor
Vice-Rector of Tashkent State University of Law



Sakari Kristian Melander
Doctor of Sciences in Law (DSc), Professor
Professor at the University of Helsinki



Khurshid Primkulovich Sadikov
Judge of the Supreme Judicial Council of the Republic of Uzbekistan



Sławomir Marek Redo
Doctor of Sciences in Law (DSc), Professor
Chairperson of the Expert Council for the Development of Scientific Research at the Faculty of Law and Administration



Vigita Vėbraitė
Doctor of Philosophy (PhD) in Law, Professor
Professor at Vilnius University



MANAGING EDITOR
Azamjon Rasuljon ugli Kambaraliev
Head Specialist at the Academy of Justice of the Republic of Uzbekistan

CONTENTS

IMPROVING THE INSTITUTION OF APPEALS: TIME LIMITS, RESPONSE QUALITY, MONITORING **10**
Achilova Liliya Ilkhomovna; Rozmetova Asal Anvarzoda

LEGAL ASPECTS OF INVESTIGATIVE JOURNALISM **18**
Jahonov Shohruh Shuhrat ugli

LEGAL BASIS OF CIVIL SOCIETY INSTITUTIONS IN THE LEGISLATION OF THE REPUBLIC OF UZBEKISTAN **25**
Sharipov Asrorjon Safar ugli

DIGITAL TRANSFORMATION OF INTERNATIONAL COMMERCIAL ARBITRATION IN UZBEKISTAN: LEGAL AND INSTITUTIONAL PROSPECTS **30**
Otakhonov Foziljon Khaydarovich

THE LEGAL NATURE OF SUBSIDIARY LIABILITY IN INSOLVENCY PROCEEDINGS INVOLVING AGRICULTURAL BUSINESS ENTITIES **39**
Rakhmatjon Tojinorovich Berdiyarov

CIVIL LAW ASPECTS OF GOODS DELIVERY BY SELF-EMPLOYED COURIERS **49**
Ruzinazarov Shukhrat Nuralievich

NATIONAL AND INTERNATIONAL EXPERIENCE IN LEGAL PROTECTION OF A COMPANY NAME: IMPROVING THE LEGISLATION OF UZBEKISTAN **63**
Allayarova Maftuna Almardanovna

ORGANIZATIONAL AND LEGAL MECHANISMS FOR COMPENSATION OF CONSTRUCTION CONTRACT DAMAGES **69**
Donayev Abduqodir Haydarovich

JURISDICTION AND VENUE OF CIVIL CASES ARISING FROM INHERITANCE RELATIONS: A NATIONAL AND FOREIGN ANALYSIS **76**
Soliyeva Kamola Rustamjon-qizi

ISSUES OF USING COURT NOTICES IN ENSURING THE OPENNESS OF CIVIL PROCEEDINGS IN COURTS **84**
Sabirov Erkinjon Kuchkarbaevich

DIGITAL EVIDENCE IN SUPPLY-CONTRACT DISPUTES BEFORE ECONOMIC COURTS: AUTHENTICATION, INTEGRITY AND EVIDENTIARY RISK IN UZBEKISTAN **91**
Mahmudova Saida Rayimjonovna

CONTENTS

FROM HUMAN CAPITAL TO INSTITUTIONAL TRANSFORMATION: A NEW STAGE IN THE STRATEGIC DEVELOPMENT OF THE JUDICIAL PERSONNEL TRAINING SYSTEM 104
Aripov Dilshod Urinbaevich

THE ROLE OF INTERNATIONAL STANDARDS IN GOVERNING ARTIFICIAL INTELLIGENCE IN JUDICIAL SYSTEMS: A COMPARATIVE AND CRITICAL ANALYSIS 109
Sadikov Khurshid Primkulovich

INDEPENDENCE — A SOLID FOUNDATION OF JUSTICE AND HUMAN DIGNITY (35 years of the evolution of the judicial and legal system of the Republic of Uzbekistan) 117
Israilov Dilshod Shavkatovich

INSTITUTIONAL MODELS OF JUDICIAL QUALIFICATION BOARDS: INTERNATIONAL STANDARDS AND FOREIGN EXPERIENCE 128
Jamolov Azizjon Nodir ugli

THE DEATH OF FREE WILL. WHO BEARS CULPABILITY WHEN ARTIFICIAL INTELLIGENCE INDUCES A PERSON TO COMMIT A CRIME? 140
Salaev Nodirbek Saparbaevich

ON EUROPEAN CRIMINAL-LAW INTEGRATION – FROM MUTUAL RECOGNITION TO LIMITED SUPRANATIONAL CRIMINAL POWER 148
Krisztina Karsai

CRIMINAL LIABILITY OF OFFICIALS OF NON-GOVERNMENTAL COMMERCIAL ORGANIZATIONS: PROBLEMS OF THEORY AND PRACTICE 158
Akramova Muazzam Turdikul qizi

DISTINGUISHING OFFENCES AGAINST SEXUAL FREEDOM FROM RELATED OFFENCES IN UZBEKISTAN 162
Achilov Izzat Tulkinovich

CRIMINAL-LAW MEASURES AGAINST THE LEGALIZATION OF PROCEEDS OBTAINED THROUGH MISAPPROPRIATION OR EMBEZZLEMENT: QUALIFICATION, EVIDENCE AND ASSET RECOVERY 170
Sadullaev Bokhodir Oybekovich

CONCEPT OF HELPLESSNESS AND ITS SIGNIFICANCE IN THE QUALIFICATION OF CRIMES 178
Khalilova Zarnigor Zafar qizi

LEGAL SIGNIFICANCE OF THE INSTITUTION OF CRIMINAL RECORDS IN PROTECTING HUMAN RIGHTS 182
Yoqubjonov Omonjon Burkhonjon ugli

CONTENTS

THE APPLICATION OF CRIMES WITH BLANKET NORMS: CURRENT STATUS AND ISSUES 189
Pulatov Bekzod Adilbaevich

THE FORMATION AND DEVELOPMENT OF THE INSTITUTION OF CRIMINAL LIABILITY IN THE FIELD OF PUBLIC PROCUREMENT: A HISTORICAL-LEGAL ANALYSIS 202
Shukurova Shahnoza Mukumjonovna

ATTORNEY'S PARTICIPATION IN THE PRE-TRIAL STAGE OF CRIMINAL PROCEEDINGS: LEGAL AND PRACTICAL ASPECTS 214
Medetbaeva Aksungul Sharapatdin kizi

INTERNATIONAL COOPERATION IN OBTAINING ELECTRONIC EVIDENCE: THE EUROPEAN PRODUCTION AND PRESERVATION ORDERS 221
Bujosa Vadell, Lorenzo Mateo

COOPERATION BETWEEN THE SUBJECTS OF INVESTIGATION IN CROSS-BORDER INTERNET FRAUD CASES 230
Khabibiddinov Nodirjon Musinjon ugli

PROBLEMS OF PROCEDURAL REALITY IN CRIMINAL PROCEEDINGS 238
Aykhan Khankishi Rustamzade, Matanat Pasha Asgarova

DETENTION OF FOREIGN NATIONAL PRISONERS IN PENITENTIARY INSTITUTIONS: A COMPARATIVE ANALYSIS OF INTERNATIONAL PRACTICES AND NATIONAL LEGISLATION 246
Rikhsimov Komron Abrorovich

CRIMINALISTIC FOUNDATIONS FOR INTEGRATING GAIT IDENTIFICATION WITH FORENSIC PORTRAIT EXAMINATION 249
Nizomova Shahrigul Karimboy qizi

INTERNATIONAL LAW CRISIS: UN PEACE OPERATIONS AND INSTITUTIONAL REFORM 258
Kudaybergenov Bakhtiyar Abdumajit-ugli

ARTIFICIAL INTELLIGENCE AND CHILDREN'S RIGHTS: PROTECTION OPPORTUNITIES AND EMERGING LEGAL RISKS 267
Ergashev Gayrat Shavkatovich

ACTIVITIES OF INTERNATIONAL NON-GOVERNMENTAL ORGANIZATIONS IN THE FIELD OF HUMAN RIGHTS 276
Nosirova Marjona Negmat kizi

Academy of Justice of the Republic of Uzbekistan
International Journal of Justice

INTERNATIONAL COOPERATION IN OBTAINING ELECTRONIC EVIDENCE: THE EUROPEAN PRODUCTION AND PRESERVATION ORDERS

Bujosa Vadell, Lorenzo Mateo
University of Salamanca, Faculty of Law
PhD, Full Professor (Catedrático), Professor of Procedural Law
E-mail: Lbujosa@usal.es
ORCID ID: 0000-0003-1660-7483



Abstract. *The expansion of digital technologies has produced a criminological reality in which the territorial element of criminal investigation is blurred: the evidence needed to prosecute both traditional offences committed online and cybercrime in the strict sense is volatile, is frequently stored outside the State conducting the proceedings and is held by private service providers. The article examines how international and, above all, European Union law has responded to this challenge, with the aim of assessing whether the new instruments reconcile the effectiveness of criminal prosecution with the fundamental rights of the persons concerned. The study applies the dogmatic-legal method, together with the historical and comparative analysis of the successive instruments on cross-border evidence, from the Council of Europe Convention on Cybercrime to the European Union regulation of 2023 on European Production Orders and European Preservation Orders and the accompanying directive on designated establishments and legal representatives. The main finding is that the principle of mutual recognition has been reshaped in a novel way, since these orders are addressed directly to private addressees rather than to the authorities of another State, which allows drastically shortened time limits but displaces onto private actors functions traditionally reserved to public authorities. The results are of practical use to judges, prosecutors and defence lawyers who must issue, enforce or challenge such orders. The article concludes that the system of safeguards is valuable but unevenly distributed, and that its real value will depend on its application in conformity with the Charter of Fundamental Rights.*

Keywords: *judicial cooperation in criminal matters; mutual recognition; cybercrime; electronic evidence; European Production Order; European Preservation Order; service providers; fundamental rights.*

Introduction

It was in the last decade of the twentieth century that a decisive impetus was given to the simplification of judicial cooperation in Europe. The Treaty of Amsterdam of 2 October 1997 and the Tampere European Council of 15–16 October 1999 are the milestones of the gradual construction of the Area of Freedom, Security and Justice; yet neither mentions, at least expressly, the need to provide assistance in respect of electronic evidentiary material, even though the Tampere conclusions already required the application of the principle of mutual recognition to pre-trial decisions so that the competent authorities could act quickly to obtain evidence.

In the twenty-odd years since then, the reality on which procedural rules operate has evolved enormously. The changes in the criminological landscape are worldwide in scope, and this must be borne particularly in mind when dealing with electronic evidence, since the territorial element becomes blurred and problems proliferate for which the traditional rules are obsolete [1, p. 325]. The problem therefore extends far beyond the European Union, but this organisation of special integration has shown a determination

to place itself in the vanguard, adopting rules that significantly update the provisions governing collaboration between bodies subject to different sovereignties.

The objective of this article is to analyse the regulation of cooperation in obtaining electronic evidence located outside the State conducting the criminal proceedings, and in particular the European Production Order and the European Preservation Order created by Regulation (EU) 2023/1543 of 12 July 2023, in order to determine whether they achieve an effective prosecution of contemporary crime without validating violations of the fundamental rights of the persons involved. That criterion is hardly original, but it cannot be relinquished: the concern that the Europeanisation of criminal justice might endanger the rule of law was voiced early [2] and remains the yardstick for evaluating every step taken to bring procedural regulation up to date.

Scholarship has long identified the evidentiary consequences of the digital transformation of crime [3, pp. 34–39; 4, p. 4] and the procedural problems of cybercrime [5; 6, pp. 22–29], while the European instruments have been examined mainly at the proposal stage [1; 11; 14; 15]. This article examines the texts as finally adopted.

Materials and Methods

The research is based on the dogmatic-legal method, applied to the analysis of the international and European instruments governing cross-border cooperation in evidentiary matters: the Council of Europe Convention on Cybercrime, done at Budapest on 23 November 2001, and its Additional Protocol of 28 January 2003; Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution of orders freezing property or evidence; Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant; Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order; Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings; and Directive (EU) 2023/1544 of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives.

This normative analysis is combined with the historical method, tracing the evolution from intergovernmental mutual assistance to mutual recognition and from analogue to digital evidence, and with the comparative method, contrasting the Budapest Convention with Union law and the new orders with the European arrest warrant and the European Investigation Order. The 2018 Commission proposals and the final 2023 texts are also compared in order to identify the systematic and substantive changes introduced during the legislative process. Doctrinal sources and the SIRIUS reports contextualise the findings.

Results

3.1. The new socio-criminal reality

The expansion of technology has been abundantly exploited to commit offences of a highly heterogeneous nature. Even without entering the deep or dark web, the most immediate layers of the digital environment are propitious for crime, and their continuous transformation complicates prosecution to the extent that the legislator has sufficient reflexes to criminalise such conduct [3, pp. 34–39]. All of this has direct consequences in the field of evidence: as has been observed, “traditional” natural and physical elements of proof have been joined by further evidentiary elements

inseparably connected to a computer or a network [4, p. 4].

The Budapest Convention contains no common definition of cybercrime; it requires signatory States to criminalise specific acts grouped in Articles 2 to 13 (offences against the confidentiality, integrity and availability of computer data and systems; computer-related and content-related offences; copyright infringements), later extended by the Additional Protocol on racist and xenophobic acts. Scholarship has proposed broader concepts: "computer crime" covers both traditional offences committed through the Internet and offences against computing itself, and may be grouped into economic cybercrime, intrusive crime and cyber-espionage or cyber-terrorism [5, p. 41]. Classifications vary according to the criterion chosen [3, pp. 47–139].

For the purposes of this study a broad conception is preferable, since the mere use of electronic channels—common to all such conduct—produces evidentiary peculiarities that must be taken into account when collecting sources of evidence in order to attribute criminal activity to specific persons, and the features of mass cybercrime point to the need for new investigative methodologies [17, pp. 197–206]. Cybercrime raises evident difficulties in determining authorship, in applying rules on jurisdiction designed for simpler contexts and even in identifying victims. Certain criminological features aggravate these difficulties [6, pp. 22–29]: computer crime can be committed with a mobile phone; the presence of the digital sphere in daily life is ever broader and more trusting; and the volume of data stored in the cloud is gargantuan, which increases the risks to everyone's rights and even to the constitutional position of the individual in a rule-of-law State [7, pp. 228–238].

3.2. Cooperation under the Budapest Convention

Effective prosecution of such extraterritorial crime requires channels of assistance from other States. The Budapest Convention—the first international treaty to address computer crime by harmonising national laws and increasing cooperation between nations [8, p. 168]—stresses in its preamble that international cooperation must be strengthened, fast and operative. Chapter III urges the Parties to cooperate to the widest extent possible for investigations concerning offences related to computer systems and data or for the collection of electronic evidence of any offence (Article 23), through extradition and, above all, mutual assistance (Articles 25–26).

Article 25(4) subjects mutual assistance to the law of the requested Party, which respects its sovereignty; Article 27(4) adds flexibility by providing that, absent applicable treaties, requests are executed according to the procedures specified by the requesting Party unless incompatible with the law of the requested Party. Of particular interest are the provisions on expedited preservation and disclosure of stored data (Articles 29–30), trans-border access to open-source data or with lawful consent (Article 32), real-time collection of traffic and content data (Articles 33–34) and the 24/7 Network of contact points (Article 35). The Convention nevertheless relies on central authorities (Article 27), and confidentiality remains optional for the requested Party (Article 28).

3.3. The evolution of European Union instruments

The first Union documents on procedural cooperation reflected the prior work of the Council of Europe, but a sui generis organisation advancing towards an ever closer union [9, pp. 47–48; 10, p. 39] had to take decisive steps towards greater fluidity among "friendly States" [18, p. 53]. That improvement is summed up in the principle of mutual recognition, formulated at Tampere as the cornerstone of European cooperation.

In the evidentiary field the evolution began with Framework Decision 2003/577/JHA on the freezing of evidence and continued with Framework Decision 2008/978/JHA on the European evidence warrant, limited to objects, documents and data and thus leaving out personal evidence. The imperfection of that regulation led to the European Investigation Order of Directive 2014/41/EU, a valuable though debated instrument [16] by which a judicial authority of the issuing State may have investigative measures carried out in the executing State to obtain evidence. But the EIO still belonged to the analogue sphere: its time limits did not correspond to the speed at which offences are committed on the Internet [11, p. 27], and differences in investigative powers between legal systems may render evidence acquired in one country inadmissible in another [12, p. 29].

Hence, on 17 April 2018, the Commission presented proposals for a Regulation on European Production and Preservation Orders (COM(2018) 225 final) and a Directive on legal representatives (COM(2018) 226 final), reaffirmed in the Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final). The third SIRIUS report confirmed the exponential growth of digital channels during the pandemic, exploited by cybercriminals, and recommended capacity-building on the instruments for obtaining electronic data from other jurisdictions [13]. After a far from simple legislative process, Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 were adopted on 12 July 2023.

3.4. The European Production Order

Article 3 of the Regulation defines the European Production Order as a decision ordering the production of electronic evidence, issued or validated by a judicial authority of a Member State and addressed to a designated establishment or a legal representative of a service provider offering services in the Union, located in another Member State. "Electronic evidence" comprises subscriber, traffic or content data stored by or on behalf of a service provider at the time of receipt of the certificate. The complexity of the subject is obvious: twenty-one definitions are set out. The order may be issued only in criminal proceedings, including those against legal persons, and for the execution of a custodial sentence of at least four months not imposed in absentia where the convicted person has absconded, and only for data relating to services offered in the Union—which will require new formulas of cooperation with third States [14, p. 294].

The subjects are the issuing and enforcing States and authorities, as in other cooperation instruments, but Article 4 graduates competence: an order for subscriber data or for data requested solely to identify the user may be issued by a judge, court, investigating judge or public prosecutor, or by another investigating authority subject to validation by one of them; an order for traffic or content data may be issued only by a judge, court or investigating judge, or by another authority

validated by them—the public prosecutor disappears in these more invasive cases. The reference to "a judge" and to "an investigating judge" as if they were different personnel is a striking inaccuracy, present in the English text too. In urgent cases an order for subscriber or identification data may be issued without prior validation, which must be sought within 48 hours. Article 7 provides that the order is transmitted directly to the designated establishment or legal representative, a genuine novelty since it is not addressed to any authority of the enforcing State [15, p. 157]; only in urgent cases, if the addressee does not react, may it be sent to any other establishment or representative of the provider in the Union.

The Regulation speaks of "conditions", but they operate as prerequisites whose absence grounds refusal (Article 5(1)). Substantively, the order must be necessary and proportionate, and a similar measure must be available in the issuing State for the same offence in a comparable domestic situation, in line with Article 6(1) of Directive 2014/41/EU. As to objective scope, an order for subscriber or identification data may be issued for all criminal offences—without even the twelve-month threshold of the European arrest warrant—whereas an order for traffic or content data is confined, through cross-references complicated for the interpreter, to offences punishable by a maximum custodial sentence of at least three years, to the offences defined in Directives (EU) 2019/713, 2011/93/EU and 2013/40/EU when committed by means of an information system, and to the terrorist offences of Directive (EU) 2017/541. Formally, Article 5(5) lists the information the order must contain (authorities, addressee, user or identifier, category and period of data, applicable criminal provisions, reasons for urgency, grounds of necessity and proportionality and a summary of the case).

The order is transmitted by means of a certificate (EPOC, Annex I) translated where necessary (Article 9). For traffic and content data the issuing authority must simultaneously notify the enforcing authority, unless the offence was committed in the issuing State or the person concerned resides there. The addressee must preserve the data and produce them within ten days, or within eight hours in urgent cases; the enforcing authority may raise grounds for refusal within ten days or 96 hours respectively. Annex III governs the dialogue when the certificate is defective, immunities or press freedom are affected or a de facto impossibility exists, the issuing authority responding within five days. Communication takes place through a secure decentralised IT system (Article 19) and a duty of confidentiality applies.

The grounds for refusal, whose systematic placement in the proposal was debatable and confusing, are now divided between Article 12 and Article 16 with non-identical content, but a general principle in favour of cooperation underlies them and they are exhaustively listed. The enforcing authority may object where the data are protected by immunities or privileges or by rules on criminal liability related to press freedom, where there are substantial grounds to believe on the basis of specific and objective evidence that enforcement would violate a fundamental right under Article 6 TEU and the Charter, where enforcement would breach ne bis in idem, or where the conduct is not an offence in the enforcing State unless it falls within the 32 categories of Annex IV punishable by at least three years; before doing so it must consult the

issuing authority, which may adapt or withdraw the order. If the addressee does not comply, the issuing authority may request enforcement (Article 16), and the addressee may object on the grounds of paragraph 4: lack of competent authority, offence outside the scope, de facto impossibility or manifest errors, data not stored at the time of receipt, service not covered, immunities and privileges, and manifest violation of fundamental rights—although, a sensu contrario from Article 16(3)(a), this last ground belongs exclusively to the enforcing authority.

As safeguards, Article 15 obliges Member States to lay down effective, proportionate and dissuasive pecuniary sanctions for non-compliance. Chapter IV establishes a review procedure where the addressee considers that compliance would conflict with the law of a third country: if the issuing authority intends to uphold the order, its competent court assesses whether that law applies and prohibits disclosure, weighing the interests protected, the connections of the case with each territory, the interests of the investigating State and the consequences for the provider. Article 18 guarantees effective remedies to all persons whose data have been requested, available to suspects and accused persons during the criminal proceedings and allowing challenges to the legality, necessity and proportionality of the measure, in addition to those of Directive (EU) 2016/680 and Regulation (EU) 2016/679.

3.5. The European Preservation Order

No less important than obtaining evidence is securing it for a subsequent request through any channel of cooperation. The European Preservation Order is a binding decision compelling a designated establishment or legal representative located in another Member State to preserve electronic evidence in view of a subsequent request for production, in the line of Framework Decision 2003/577/JHA and of the expedited preservation already provided in the Budapest Convention. It applies to the same proceedings and the same data as the production order, but its subjective regime is simpler: it may be issued, for any category of data, by a judge, court, investigating judge or public prosecutor, or by another investigating authority subject to their validation. The assessment of necessity and proportionality is here related to preventing the removal, deletion or alteration of data, and the order may be issued for all offences for which it would be available in a similar domestic case. The preserved data may later be requested by mutual legal assistance, an EIO or a European Production Order.

The order is transmitted through a certificate (EPOC-PR, Annex II); the addressee must preserve the data without undue delay for sixty days, extended if the issuing authority confirms that a request for production has been launched. The consultation mechanisms of Annex III apply, and the addressee may object only on exhaustive grounds parallel to those of the production order. Pecuniary sanctions apply equally, but the provisions on effective remedies and on the review of conflicting obligations are expressly confined to production orders.

3.6. Designated establishments and legal representatives

Directive (EU) 2023/1544 supplies the addressee that the orders presuppose. Its Article 3 obliges Member States in which providers offer services to ensure that they designate at least one addressee for the receipt of, compliance with and enforcement of decisions and orders for gathering electronic evidence under the Regulation, Directive

2014/41/EU and the 2000 Convention on Mutual Assistance, as well as under national law. Providers established in the Union must designate one or more establishments; those not established must appoint legal representatives; and providers in non-participating Member States must do the same if they offer services in participating States.

Discussion

The principle of mutual recognition, the driving force of European cooperation since Tampere, continues to bear fruit, but has been reshaped in a way earlier instruments did not anticipate. In the European arrest warrant, the freezing order and the EIO the relationship was always between authorities; the new orders are addressed to private addressees, which is what makes it possible to reduce time limits to ten days or eight hours, but also transfers to service providers assessments—on immunities, on manifest errors, on de facto impossibility—that were traditionally reserved to public authorities. This is the most significant novelty of the system [15, p. 157] and its principal risk.

Compared with the Budapest Convention, the Union has dispensed with central authorities, with the political-offence exception and, for subscriber data, with any threshold of seriousness, in line with the reasonable widening of mutual recognition beyond serious crime. In exchange it has strengthened guarantees the Convention left optional: confidentiality, judicial reservation for traffic and content data, notification of the enforcing authority, exhaustive grounds for refusal including a fundamental-rights clause, and effective remedies. The comparison between the 2018 proposal and the 2023 text also shows improvements—the correction of the confusing placement of the grounds for refusal, the addition of a four-month threshold for enforcement of sentences—together with persisting defects: the inaccurate terminology on judicial authorities, the complicated cross-references delimiting the scope for traffic and content data, and the duplication of grounds for refusal in two chapters with non-identical content.

Two shortcomings deserve emphasis. First, the remedies of Article 18 and the review procedure for conflicting obligations are confined to production orders, leaving the preservation order in a weaker position; yet the preservation of data is not a matter of indifference to data subjects, as the extensive development of data protection in the Union itself makes plain. Second, the requirement that a similar measure be available in the issuing State in a comparable domestic case presupposes a harmonising effort that, if absent, may block requests and frustrate the fundamental right to evidence. More broadly, the exclusively European character of the orders confirms the need for new formulas of cooperation with third States [14, p. 294], where much of the data relevant to European proceedings remains located. These difficulties, together with divergent national rules on admissibility [12, p. 29], mark the limits of what the new instruments can achieve on their own.

Conclusion

Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 are a decisive step towards the effective prosecution of contemporary crime, adapting the principle of mutual recognition to a reality in which evidence is volatile, extraterritorial and held by private operators. The most striking novelty—the direct addressing of orders to designated establishments and legal representatives—is

also the feature that requires the greatest vigilance, since it displaces onto private actors functions of public authorities. The safeguards surrounding the system (necessity and proportionality, judicial reservation for the most intrusive orders, notification of the enforcing authority, exhaustive grounds for refusal, review of conflicting obligations, sanctions and effective remedies) are valuable but unevenly distributed. Member States should extend effective remedies to preservation orders, ensure that the "comparable domestic situation" requirement does not obstruct cooperation, and train practitioners in the new instruments. The real value of the orders will be measured by their application in conformity with Article 6 TEU and the Charter of Fundamental Rights and by the Union's success in articulating comparable cooperation with third States.

References

1. Bueno de Mata F. Análisis crítico de las futuras órdenes europeas en materia de prueba electrónica [Critical analysis of the future European orders on electronic evidence]. In: Bueno de Mata F. (ed.). La cooperación procesal internacional en la sociedad del conocimiento. Barcelona, 2019, p. 325 ff.

2. Schünemann B. ¿Peligros para el Estado de Derecho a través de la europeización de la administración de justicia penal? [Dangers to the rule of law through the Europeanisation of criminal justice?]. In: Armenta Deu T., Gascón Inchausti F., Cedeño Hernán M. (eds.). El Derecho procesal penal en la Unión Europea. Tendencias actuales y perspectivas de futuro. Madrid, 2006.

3. Miró Llinares F. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio [Cybercrime. Phenomenology and criminology of crime in cyberspace]. Madrid, 2012.

4. Ziccardi G. Le tecniche informatico-giuridiche di investigazione digitale [Legal-computing techniques of digital investigation]. In: Lupária L., Ziccardi G. (eds.). Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milan, 2007, p. 4 ff.

5. Velasco Núñez E. Delitos cometidos a través de internet. Cuestiones procesales [Offences committed through the Internet. Procedural questions]. Madrid, 2010.

6. Ortiz Pradillo J.C. Problemas procesales de la ciberdelincuencia [Procedural problems of cybercrime]. Madrid, 2013.

7. Armenta Deu T. Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambios [Drifts of justice. Protection of rights and dispute resolution in times of change]. Madrid, 2021.

8. Fernández Bermejo D., Martínez Atienza G. Ciberseguridad, ciberespacio y ciberdelincuencia [Cybersecurity, cyberspace and cybercrime]. Cizur Menor, 2018.

9. Mangas Martín A., Liñán Nogueras D. Instituciones y Derecho de la Unión Europea [Institutions and Law of the European Union]. 10th ed. Madrid, 2020.

10. Schütze R. European Union Law. 2nd ed. Cambridge, Cambridge University Press, 2018.

11. Bueno de Mata F. Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen [Analysis of international judicial cooperation measures for the cross-border obtaining of evidence in cybercrime matters]. In: Fontestad Portalés L. (ed.). La transformación digital de la cooperación jurídica penal internacional. Cizur Menor, 2021, p. 27 ff.

12. Biasiotti M.A. Present and Future of the Exchange of Electronic Evidence in Europe. In: Handling and Exchanging Electronic Evidence Across Europe. Cham, Springer, 2018, p. 29 ff.

13. Eurojust, Europol. SIRIUS EU Digital Evidence Situation Report 2021. Available at: https://www.eurojust.europa.eu/sites/default/files/assets/sirius_eu_digital_evidence_situation_report_2021.pdf (accessed: 07.01.2022).

14. Fuentes Soriano O. Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas [Europe facing the challenge of digital evidence. Common evidentiary instruments: the European production and preservation orders for electronic evidence]. In: Fuentes Soriano O. (ed.). Era digital, sociedad y Derecho. Valencia, 2020, p. 294 ff.

15. Gómez Amigo L. Prueba penal electrónica en la Unión Europea: las futuras órdenes europeas de entrega y conservación [Electronic criminal evidence in the European Union: the future European production and preservation orders]. In: González Cano M.I. (ed.). Orden Europea de Investigación y prueba transfronteriza en la Unión Europea. Valencia, 2019, p. 157 ff.

16. Moreno Catena V., Romero Pradas M.I. (eds.). Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof.ª M.ª Isabel González Cano [New postulates of judicial cooperation in the European Union]. Valencia, 2021, pp. 477–706.

17. Sánchez-Rubio A. Cooperación policial y judicial en la prevención y represión de delitos mediante diligencias de investigación tecnológicas [Police and judicial cooperation in the prevention and repression of offences through technological investigative measures]. In: Bueno de Mata F. (ed.). La cooperación procesal internacional en la sociedad del conocimiento. Barcelona, 2019, pp. 197–206.

18. Palomo del Arco A. Convenio 2000. Ámbito de aplicación y relación con otros convenios [The 2000 Convention. Scope and relationship with other conventions]. In: Galgo Peco A. (ed.). Derecho penal supranacional y cooperación jurídica internacional. Cuadernos de Derecho Judicial. Madrid, 2004, p. 53 ff.

