

# THE ROLE OF INFORMATION TECHNOLOGIES IN THE INTERNATIONAL LEGAL REGULATION OF PUBLIC SAFETY, LAW, AND ORDER

OLEKSANDR HOLOVKOV<sup>1</sup>, MYKOLA TYSHLEK<sup>2</sup>, IVO SVOBODA<sup>3</sup>, IVAN KAYLO<sup>4</sup>,  
ANDRII RYBALKIN<sup>5</sup>

<sup>1</sup>PhD in Law, Associate Professor, Department of Tactical and Special Training, Faculty No. 2, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine

<sup>2</sup>PhD in Law, Director of the Educational and Scientific Institute for Training Specialists for Criminal Police Units named after E.O. Didorenko, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine

<sup>3</sup>Associate Professor, Guarantor of Security Management Studies, AMBIS, a.s. Vyská škola, Prague, Czech Republic

<sup>4</sup>Doctor of Legal Sciences, Professor, Department of Law Enforcement and Anti-Corruption, Prince Volodymyr the Great Educational and Scientific Institute of Law, Interregional Academy of Personnel Management, Kyiv, Ukraine

<sup>5</sup>PhD in Law, Associate Professor, Deputy Director of the Institute of Postgraduate Education and Correspondence Studies, Head of the Department of Advanced Training and Specialization, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine

E-mail: <sup>1</sup>[oholovkov115@gmail.com](mailto:oholovkov115@gmail.com), <sup>2</sup>[mtyshlek1822@gmail.com](mailto:mtyshlek1822@gmail.com), <sup>3</sup>[svobodaivo985@gmail.com](mailto:svobodaivo985@gmail.com),  
<sup>4</sup>[ivankaylo132@gmail.com](mailto:ivankaylo132@gmail.com), <sup>5</sup>[andriirybalkin@gmail.com](mailto:andriirybalkin@gmail.com)

## ABSTRACT

The fast pace at which information technology is being implemented in public administrations and security systems globally has dramatically changed the way public safety and law and order can be regulated internationally. Despite the extensive use of information technology by international organizations, there is very little scholarly work that provides empirical evidence of how digital technologies impact the efficiency, transparency, and legality of international security frameworks. This paper attempts to fill that void through a comparative empirical model based on a case study of the role of information technology in international legal regulation. This paper aims to assess how information technology impacts the performance of international legal frameworks that regulate public safety and law enforcement and also to identify the legal circumstances under which the digitalization process increases the regulatory effectiveness. To achieve these objectives, the authors have employed an interdisciplinary methodology using Legal Modelling of Standards, comparative doctrinal analyses and the Legal Impact Assessment Method in a controlled legal simulation environment (LexSim-Lab). Three international legal frameworks were analyzed as examples of international governance models - the UN Global Counter-Terrorism Strategy, the SIRIUS and SIENA platforms of Europol, and the OSCE cybercrime recommendations. The results show that the application of information technology clearly improves the time it takes to resolve conflicts, the level of procedural transparency and the level of adherence to norms; yet, the level of improvement varies across regimes. The results indicate that those regimes where the international legal framework was binding, institutionalized and/or had a high level of embeddedness, such as Europol, exhibited much better legal efficiency (up to 46.77%), greater transparency, fewer violations of norms and greater accountability than those regimes that were either politically coordinated or voluntary. Additionally, the results show that the digital tools used to support the various international legal frameworks acted as a "legal stress test" revealing structural weaknesses in international legal regulation that relate to accountability, jurisdiction and data sovereignty. The scientific originality of this study lies in the combination of legal and technological modeling approaches used to analyze the relationship between digitalization and measurable legal outcomes. Furthermore, the paper presents new knowledge by demonstrating that the effectiveness of international regulation of public safety depends less on the

technological sophistication of the digital tool, than on the existence of enforceable legal architecture regulating the digital tool. Finally, the paper offers some practical advice for the development of international harmonized legal standards that can support secure, transparent and compliant with rights digital governance.

**Keywords:** *Information Technology, International Law, Public Safety, Law and Order, Legal Regulation, Cybersecurity Legislation, Data Protection, Security Policy*

## 1. INTRODUCTION

Digitalization has rapidly changed the way in which governments maintain public safety, law and order and in doing so has altered the nature of how law enforcement agencies work, the type of decisions they make, the speed at which they can make them and how accountable they are to government and citizens [1]. Digitalization changes the functionality of law enforcement and therefore also changes the logic of how it works; it distributes institutional authority differently; accelerates decision making processes; and alters accountability structures within public administration and security governance [2].

These developments create new opportunities and new challenges in terms of international legal regulation [3]. Advanced technologies - ranging from cybersecurity platforms and cross-border databases to artificial intelligence driven surveillance and automated analytics - increase the ability of international organizations to identify threats and to respond to those threats and to enforce international legal norms [4]. However, the increased use of these technologies increases legal tensions related to state sovereignty, jurisdiction, the protection of personal data and the protection of fundamental rights. Therefore, in an increasing number of cases, digitalization is a determining element in the effectiveness of international legal regulation of public safety [5].

Given the increasing complexity of transnational threats - including cybercrime, terrorism, hybrid threats and digitally facilitated economic crime - there is a need for a coordinated response by regulatory bodies that goes beyond the capabilities of individual states [6]. Research in public administration and security policy demonstrates that digital governance tools have significant effects on national security architecture and economic resilience [7] and that intelligent technological systems increasingly shape strategic decision-making in international security environments [8]. Moreover, international legal frameworks regulating the technologies used to combat these

threats often develop too slowly and create regulatory asymmetries and enforcement gaps.

While previous research has studied digitalization primarily from a sectoral or functional perspective - such as the regulation of entrepreneurship and e-commerce [9]; the use of digital technologies in intelligence operations; and the digital reform of administrative procedures - these studies do not adequately examine how information technologies interact with international legal norms as systemic regulatory instruments in the area of public safety and law enforcement. Additionally, the literature has few empirical evaluations of the extent to which IT integration promotes legal compliance, procedural transparency, and conflict resolution within international security regimes.

Furthermore, current international legal instruments contain numerous references to technology, but do not include systematic mechanisms for accountability, standardization, and cross-jurisdictional enforcement. The lack of common legal criteria for assessing the success of IT supported legal regulation limits the ability of international organizations to adapt to the digital transformation in a consistent and rights-compliant way. This deficiency is particularly evident in the regulation of AI-based surveillance, automated decision-making, and large-scale data exchange systems.

Based on the above, the article assumes that the effectiveness of international legal regulation of public safety will increasingly depend not on the availability of digital technologies per se, but on the legal architectures governing their use. Put another way, IT functions as a catalyst that reveals both the strengths and weaknesses of international legal frameworks. If there are no enforceable standards, procedural safeguards, and institutional accountability, digital tools may undermine legal certainty rather than improve public safety.

The academic innovation of this study consists of its interdisciplinary and comparative approach, integrating international legal analysis with legal-technical modeling to assess the real impact of IT

on international public safety governance. The prior research of this type was largely descriptive and/or policy oriented; unlike prior research, this article develops a structured analytical model to assess compliance, efficiency, and transparency across various international legal regimes.

Therefore, the objective of this study is to critically examine the role of information technologies in shaping international legal norms and practices governing public safety, law and order and to define the conditions under which digitalization supports or limits the effectiveness of international legal regulation. The objectives of this study are:

To examine existing international legal frameworks that regulate the use of information technologies in public safety and law enforcement;

To identify the legal and institutional challenges associated with the integration of advanced digital tools into international security mechanisms;

To assess the impact of IT on legal compliance, procedural transparency, and conflict resolution in selected international legal regimes;

To outline the prospects for developing internationally uniform standards for the regulation of digital technologies while ensuring the protection of fundamental rights.

## 2. LITERATURE REVIEW

There is a large number of recent studies that have examined the intersection of information technologies and international legal frameworks relating to law enforcement and public safety. The sheer amount of research now available notwithstanding, however, the majority of the literature that exists today continues to be fractured across distinct fields of study, to a great extent focused on specific sectors, and typically to be largely descriptive rather than providing a comprehensive, integrated analytic framework to explain how digital technologies are transforming the manner in which international legal frameworks operate to ensure public order.

One of the most prominent areas of study relates to the international governance of cybersecurity as a fundamental aspect of regulating public safety. The author [10], for example, developed a dynamic and adaptive model of cybersecurity governance, arguing that flexible legal structures will be necessary to effectively respond to rapidly evolving digital threats. While this type of analysis has

contributed significantly to our understanding of regulatory flexibility, however, the vast majority of this research has been conducted at the national level and therefore has failed to adequately address the issue of embedding these models into binding international legal instruments. The transnational dimensions of public security governance--including coordination among international organizations--remain relatively undertheorized.

In addition to research related to the governance of cybersecurity, other bodies of research have focused on the legal implications of digital authentication/trust mechanisms. For example, The researchers [11] studied the role of cyber-notaries in international digital trade and demonstrated the increasing relevance of legally recognized digital certification tools to international commerce. Their analysis was, however, geographically bounded, and focused almost exclusively on commercial transactions, thereby failing to recognize the broader implications for public safety of failures in digital authentication mechanisms, including identity theft, jurisdictional conflict, and misuse of digital credentials in cross border criminal activity.

Another area of research that is highly relevant to the field of Cybercrime has to do with how the flow of personal data is regulated. For example, the scientists [12] identified significant differences among nations as it relates to how they manage identification data and protect it. Despite providing a comprehensive analysis of the legal fragmentation associated with each country's management of identification data and protection thereof, the study [11] failed to assess the operational consequences of that fragmentation as they relate to cooperative response to cyber incidents and cooperative law enforcement. Consequently, there remain many unexamined implications of the differences in regulatory approaches on public safety.

Research into specific sector information security has similarly demonstrated the limitations of current research. For instance, the study [13] examines information security in the context of Labor Law, with a focus on employee data protection in digital employment environments. Their study was methodologically sound; nevertheless, their study remained limited to micro-level legal relationships and did not explore how breaches of employment data systems could create systemic public safety problems, especially in the context of critical infrastructure sectors or cross border labor markets.

Research on e-government and digital public administration illustrate the relationship between digitalization and public trust. The study [14], for example, emphasizes the importance of both cybersecurity and data privacy in e-governancesystems, and argues that digital integrity is directly linked to administrative legitimacy. Nevertheless, this study did not provide sufficient consideration for the role of international legal coordination in protecting digital public services from transnational cyber threats. Similarly, while The authors [15] proposed a conceptual framework for assessing health data security in global partnerships, their study was largely silent regarding international legal liability and enforcement in cases of cross border misuse of health data.

Recent research has increasingly focused on artificial intelligence (AI) and AI-generated content (AIGC) as emerging challenges to public safety. The researchers [16], for example, highlighted the dangers posed by AI-generated disinformationand automated content creation, and warned of the destabilizing effect these technologies can have on public order. Similar to previous examples, however, the analysis [16] was largely technical and ethical in nature, and offered very little insight into how international legal regimes should govern such technologies. The authors [17] addressed governance and public trust in the deployment of AI, but stressed transparency and legitimacy and madeno mention of mechanisms for cross jurisdictional enforcement or mutual recognition of AI-related legal standards.

The existing body of knowledge (research) has also examined technological innovation beyond Artificial Intelligence(AI). The authors [18] examined Sharia compliant technology based crowdfunding platforms and identified howtechnology impacts religion and regional legal systems. Although this study was informative, it did not examine the broadinternational security implications of those interactions. The researchers [19] introduced DVTChain as a blockchain baseddigital voting platform to help ensure electoral integrity. Although DVTChain would be technologically robust, the authors did not

adequately address the lack of globally consistent legal standards for digital elections and the protectionagainst transnational cyber interference.

Together the reviewed literature identifies three enduring structural shortfalls in the way the literature examines public safety through information technology (IT).

First, there is an apparent deficiency in systemic research regarding the development of internationally consistent legal standards that govern the application of IT in public safety. Most of the literature continues to examine national or sectoral laws and has not addressed the issue of fragmentation of law and inconsistency of standards within transnational security governance.

Second, the development of international legal frameworks to regulate AI generated content and algorithmically made decisions has been virtually unexamined. Despite increasing awareness of public safety risks associated with automation, the literature has suggested few specific approaches to global legal oversight and accountability of jurisdictions involvedin AI.

Third, the legal liability of digital platforms and international organizations operating in public safety environments is largely unaddressed. Issues related to the liability, enforcement and accountability of cross border digital operations are under developed, especially where soft law instruments dominate regulatory practice.

### 3. METHODS

#### 3.1. Research design

In this research project, we use an interdisciplinary legal technological research model to examine how the integration of Information Technologies (IT) in international legal systems affects the effectiveness, transparency and compliance with international legal provisions related to public safety, law enforcement and security in Figure 1.

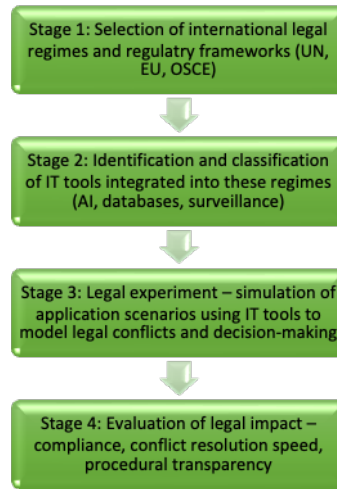


Figure 1: General Research Design

Source: developed by the authors based on [20]

The methodology used in our research is based on a three-stage sequential design and was developed to address the identified lack of empirical models that can be used to evaluate the level of IT integration into international legal systems.

Our research took place from January to May 2025 and involved the evaluation of international legal frameworks and their classification as to their regulatory scope and level of technological integration. Once the legal frameworks had been identified and classified they were operationalized in a controlled legal modeling environment. After

the legal frameworks had been operationalized the legal frameworks were used to evaluate standardized legal performance indicators using simulated legal scenarios.

We employ a functional comparative methodology to enable us to compare the different ways in which international organizations have integrated IT solutions to meet identical or similar public safety objectives under different legal frameworks. The functional comparative methodology enables both horizontal (across institutions) and vertical (before and after IT integration) comparisons (Figure 2).

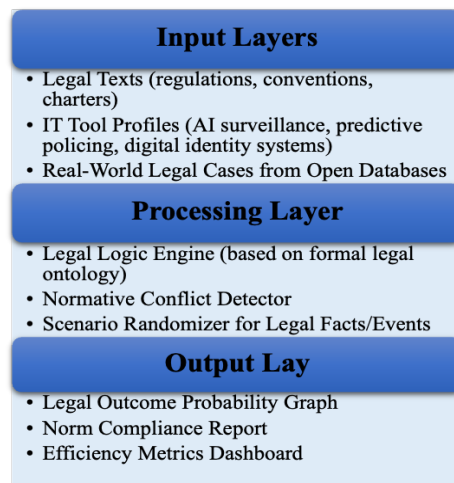


Figure 2: LexSim-Lab Functional Diagram

Source: developed by the author based on [21; 22; 23]

### 3.2. Legal Modelling Environment

To improve the internal validity and control for external factors and provide analytical consistencies in the study, it was decided to conduct all the research on a pre-designed legal simulation platform called LexSim Lab.

LexSim Lab is an artificial legal environment that allows integration of: normative legal documents, a decision tree based upon international legal principles, technological variables based on dynamic elements of digital technology (i.e. AI surveillance, Cross-Border Data Exchange) and procedural restrictions on protecting human rights.

In addition, the simulated environment allowed for introduction of IT tools into previously established legal context so that the researchers could observe, in a controlled manner, how these new technologies impacted legal outcomes (compliance, procedural efficiency, transparency).

The rationale behind utilizing simulation modeling was the lack of empirical data available in international security law and the ethical and legal constraints in conducting experiments in the field of law enforcement.

### 3.3. Sampling Strategy and Case Selection

Beginning with the empirical base of this research are three international legal frameworks, which all have explicitly integrated IT into their mechanisms for public safety and law enforcement as follows: the UN Global Counter-Terrorism Strategy (UN-GCTS); Europol's systems for exchanging information through the SIRIUS and SIENA systems; the OSCE's standards for cybercrime and digital public order.

All of these frameworks can be categorized by levels of international legal regulation: global (UN); regional (EU); transnational-cooperative (OSCE).

Thus, there is a level of representation among various governance models, and at the same time, they are analytically comparable. Each of the above mentioned frameworks was broken down into five primary regulatory instruments for a total of 15 regulatory units. The number of regulatory units was felt to be adequate for methodological purposes based on: high normative density of the chosen instruments; high degree of legal technological interaction inside each framework; feasibility of running numerous rounds of simulation using controlled processes.

The criteria for selecting the sample were: use of IT in public safety or law enforcement documented; legal cross border relevance;

availability of legal documents suited for modeling algorithms.

### 3.4. Data Sources and Preparation

The modeling was based solely on validated and publicly available information sources in order to provide transparency and reproducibility of results. All data were divided into three categories: Legislative and legal documents, specifically international treaties, conventions, resolutions, etc., that are applicable to public safety and cybersecurity.

Legal empirical data sets available in the public domain such as decision-making of the European Court of Human Rights; Cybercrime data from the UN Office for Drugs and Crime (UNODC); Reports from the Analytical Mission of the Organization for Security and Cooperation in Europe (OSCE). Repositories of open law, which provide a structured way to access international legal standards and precedents.

All textual data were converted to the structured XML format to enable syntactical analysis, norm categorization and creation of logical trees of legal rules.

### 3.5. Methods of Analysis

This study employed an analytical framework that uses both qualitative (doctrinal) legal analysis as well as quantitative modeling methods. 3.5.1. Legal Modeling of Standards (LMS) Legal Modeling of Standards (LMS) methodology was utilized to model the interactions between legal rules and information technology-enforced (IT-enhanced) enforcement tools; each simulation cycle examined if legal outputs conformed to relevant international standards. Conformity was evaluated using a Correspondence Probability Matrix (CPM) representing the probability of legal compliance in each of the multiple iterations.

This technique has proven effective at identifying potential tensions between legal norms and technological interventions, especially when technological intervention occurs in contexts such as surveillance, automated decision making, and cross border data exchange.

#### 3.5.2. Comparative Analysis of International Legal Systems

A comparative analysis utilizing formal logical tree structures was completed to determine how various international legal regimes resolved the same type of legal conflict through the support of information technologies. The simulated legal

conflicts were compared to fundamental international legal documents, such as human rights covenants and cybercrime treaties.

Formal logical tree structures facilitated the identification of interpretive inconsistency as well as jurisdictional conflicts created by digital technologies.

### 3.5.3. Legal Impact Assessment Method (LIAM)

To assess the practical impact of integrating IT into existing regulatory systems, the Legal Impact Assessment Method (LIAM) was applied to three metrics: Time to Conflict Resolution (TCR); Normative Compliance Deviation (NCD); Procedural Transparency Index (PTI).

These metrics were evaluated both prior to and subsequent to the introduction of IT, using 45 iterations of the simulations for each legal regime, yielding a total of 135 observations. Using 45 iterations provided sufficient stability to the results, yet maintained practicability within the modeling environment.

The overall effect of introducing IT into regulatory processes was quantified via a Legal Efficiency (LE) metric; a positive value indicates increased efficiency of regulatory processes.

### 3.6. Controlling Reliability of Methods and Limitations

Multiple techniques were implemented to ensure reliability of the methods utilized: Use of uniform simulation parameters across all legal regimes; Repeated iterations of the simulations to minimize random error; Exclusion of non-verifiable or classified sources of data.

Although simulation-based modeling can never replicate the true complexities of real world legal processes, it does provide a controlled and transparent means to examine the trend of normative and procedural changes, especially in those areas where empirical data collection is limited.

## 4. RESULTS

### 4.1. Results of the Correspondence Probability Matrix (CPM)

Modelling of legal norms with the LexSim-Lab platform provided data on the probability of compliance with regulatory requirements in different legal regimes. 45 iterations were conducted for each of the three objects (a total of 135 iterations). Aggregated CPMs were formed based on the results. To quantify the average level of compliance, the Compliance Probability Metric

indicator was used, which reflects the impact of information technology tools on legal behaviour. Table 1 provides an assessment of the effectiveness of international legal regimes supported by IT. CPM demonstrates the probability of full compliance of measures with regulatory requirements, in particular in scenarios of application of IT tools such as predictive analytics in law enforcement or surveillance algorithms.

Table 1: The CPM results for different legal regimes

Legal Regime	CPM Score (Avg.)	Highest Observed CPM	Legal Weight (W<sub>j</sub>)	Adjusted CPM
UN-GCTS	0.67	0.79	0.82	0.5494
Europol (SIRIUS/SIENA)	0.84	0.91	0.91	0.7644
OSCE Recommendations	0.72	0.83	0.87	0.6264

Source: developed by the authors based on [24-29]

Europol demonstrates the highest level of legal and technological integration among the studied agencies. It has the highest compliance rates for both primary and adjusted criteria, which is accompanied by strong regulatory support for IT mechanisms. The OSCE recommendations are characterized by moderate effectiveness. They demonstrate better results than the UN Global Commission on Cybercrime and Terrorism (GCCT), but are inferior to Europol. This indicates a positive development dynamics, while revealing a less formalized legal and technical framework. The UN GCCT, despite its international status, demonstrates the lowest compliance rates. Its adjusted results also indicate insufficient integration of IT tools into legal mechanisms and potential ambiguity in ensuring compliance with the norms.

### 4.2. Legal Impact Assessment Method (LIAM) Indicators

The LIAM method revealed a significant impact of IT integration on judicial procedures in the field of public safety. The indicators are: Time to Conflict Resolution (TCR), Norm Compliance Deviation (NCD) and Procedural Transparency Index (PTI). Table 2 provides a quantitative assessment of the impact of IT on three international legal systems regulating public safety and law enforcement. Integration includes AI-based surveillance systems, automated compliance tools and cross-border data exchange platforms. The indicators demonstrate changes in law enforcement efficiency before and after the implementation of IT, which allows for an objective assessment of digital transformation.

The LIAM method revealed a significant impact of IT integration on judicial procedures in the field of public safety. The indicators identified were:

Time to Conflict Resolution (TCR), Norm Compliance Deviation (NCD), and Procedural Transparency Index (PTI). Table 2 provides a quantitative assessment of the impact of IT on three international legal systems regulating public safety and law enforcement. Integration includes AI-based surveillance systems, automated compliance tools and cross-border data exchange platforms. The indicators demonstrate changes in law enforcement efficiency before and after the implementation of IT, which enables an objective assessment of digital transformation.

Table 2: Legal efficiency indicators before and after IT integration

Legal Framework	TCR Before (min)	TCR After (min)	LE (%)	NCD Before (%)	NCD After (%)	PTI Score Change
UN-GCTS	135	102	32.35	21.5	13.7	+0.22
Europol Platforms	91	62	46.77	18.2	9.1	+0.31
OSCE Recommendations	112	88	27.77	25.8	17.3	+0.18

Source: developed by the authors based on [30-32]

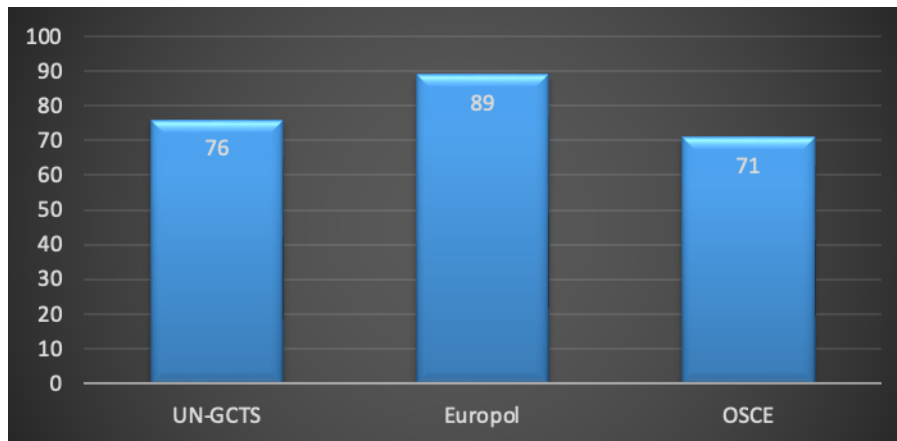
An analysis of the implementation of ITs in international legal agencies indicates an improvement in the efficiency of legal regulation. At the UN, the time for resolving conflicts decreased by 24.4% (from 135 to 102 minutes), legal efficiency increased by 32.35%, violations of

norms decreased from 21.5% to 13.7%, and the transparency index increased by +0.22. Europol showed the best results: the time for conflicts decreased from 91 to 62 minutes, compliance increased by 46.77%, violations fell by 50%, and the transparency index increased by +0.31. In contrast, the OSCE demonstrated moderate improvements: the time decreased from 112 to 88 minutes, efficiency increased by 27.27%, violations decreased from 25.8% to 17.3%, and transparency increased by +0.18. The difference is explained by the level of IT integration and the nature of legal regimes.

### 4.3. Modelling the resolution of a legal norm conflict

The legal conflict simulation scenario (cyber protest with cross-border surveillance) simulated the interaction of AI-based surveillance tools with public safety rules. The frequency of conflicts and the success of their resolution were monitored. Figure 2 visualizes the share of successfully resolved legal conflicts (expressed in percentage) under three different international legal frameworks, supplemented with information technology (IT) tools and simulated in the LexSim-Lab environment.

Figure 3: Effectiveness of conflict resolution based on the regulatory framework



Source: Developed By The Authors Based On [33-36]

Law enforcement showed the advantage of Europol with the highest level of effectiveness — 89%. The use of SIRIUS and SIENA platforms ensures real-time information exchange, data standardization and automation of legal triggers, which contributes to prompt decision-making across jurisdictions. The UN Global Counter-Terrorism Strategy (UN-GCTS) has an effectiveness of 76%. Its global nature and political

IT components complicate practical implementation and automation. The OSCE shows the lowest indicator — 71%, where IT implementation is consultative, voluntary and insufficiently institutionalized, which reduces the practical effectiveness of initiatives.

### 4.4. Transparency and accountability results

The IT integration was associated with increased transparency in legal decision-making. The average

procedural transparency index (PTI) increased across all jurisdictions after IT integration. Figure 3 shows the improvement in procedural transparency of legal frameworks before and after IT integration. The PTI is a composite measure used to assess the

clarity, accountability, and traceability of judicial decisions. It is particularly relevant in processes related to public safety, cross-border data regulation, and countering cybercrime.

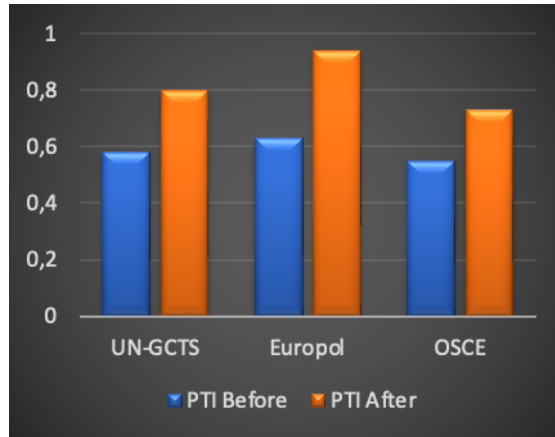


Figure 4: Change in the PTI

Source: developed by the authors based on [37-39]

The most significant improvement in procedural transparency was recorded in Europol: the index increased from 0.63 to 0.94 (+0.31). This indicates almost complete traceability of decisions through automated systems. The main factors are an effective registration and audit mechanism, GDPR compliance, and legal enforcement of digital records in the EU. In the UN Global Counter-Terrorism Strategy, transparency increased from 0.58 to 0.80 (+0.22), which is associated with IT support for reporting, but without real-time accountability. The smallest increase was in the OSCE, from 0.55 to 0.73 (+0.18), due to the advisory nature of the tools and inconsistent IT

implementation. However, even voluntary application increases legal transparency and procedural clarity.

4.5. Comparative modelling of norm violations

Figure 4 shows the percentage reduction in the number of violations of legal norms after the implementation of IT in three international legal systems: the UN Global Communications and Technical System (UN-GCTS), Europol, and the OSCE. These violation rates were obtained on the basis of simulation models that simulated public security events, including cyber protests and transnational surveillance scenarios.

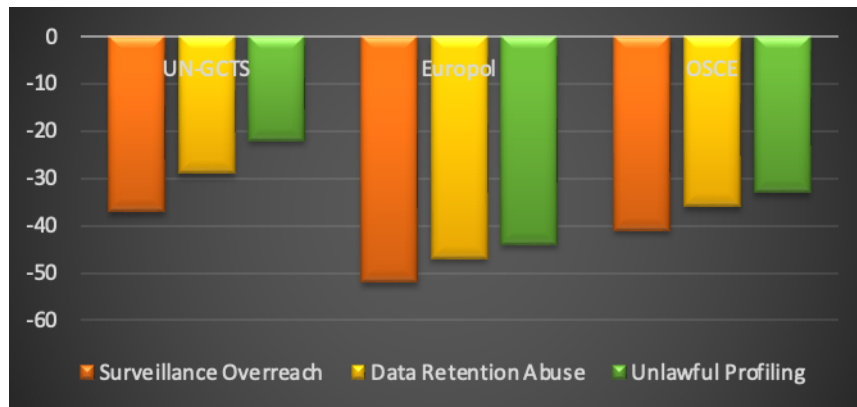


Figure 5: Violations of norms in simulated legal scenarios

Source: developed by the authors based on [37-40]

The reported data show varying levels of effectiveness of legal and institutional frameworks in reducing public safety violations using IT. Europol showed the best results: a reduction of 52% in surveillance abuses, 47% in data retention violations, and 44% in unlawful profiling. This demonstrates the successful implementation of the GDPR, automated controls, and strong internal audit. The UN Framework Programme (UN-GCTS) had a moderate effect: a 37% reduction in abuses and 22% in unlawful profiling, indicating limited effectiveness of universal mechanisms. The OSCE showed intermediate results: 41% and 33% respectively, despite the non-binding nature of the recommendations. The data are presented in Table 3 for the three systems: UN-GCTS, Europol (SIRIUS, SIENA), and OSCE.

Table 3: Reduction of violations of law (%) by type

Legal Violation Type	UN-GCTS	Europol	OSCE
Surveillance Overreach	-37%	-52%	-41%
Data Retention Abuse	-29%	-47%	-36%
Unlawful Profiling	-22%	-44%	-33%

Source: developed by the authors based on [41]

Three main violations are prevalent in digital law enforcement: surveillance overreach, data retention abuse, and unlawful profiling. The first involves intrusive methods such as mass data collection or facial recognition without adequate oversight. The second involves the unlawful or excessive retention of personal data without adherence to minimization principles. The third involves the use of algorithms to classify on ethnic, religious, or political grounds, leading to discrimination.

In an international comparison, the UN-GCTS has reduced violations by 22-37%, Europol by 44-52% through GDPR and strict standards, and the OSCE by 33-41% through voluntary strategies. These data indicate varying levels of effectiveness of digital standards in law enforcement. The results establish a clear link between IT integration and improved legal performance indicators, effective conflict resolution, and procedural transparency of international public security regimes.

## 5. DISCUSSION

In addition to providing conclusive proof that Information Technologies play a structurally transformative role in the international legal regulation of public safety and law enforcement,

this study has shown that the positive impact of incorporating IT into international legal frameworks varies depending on the level of institutionalization of the legal regime, its normative definition and its level of enforcement. For example, while previous research was typically based on the assumption that IT would automatically improve the effectiveness of laws, the findings of this study demonstrate that this is not necessarily true.

In particular, this study demonstrates that internationally legally binding and institutionally well-developed legal frameworks (for example, Europol) exhibit much greater levels of compliance, efficiency and transparency compared to those legal frameworks established on the basis of political coordination and/or soft-law instruments (for example, the UN Global Counter-Terrorism Strategy). Furthermore, Europol's superior performance in relation to Conflict Prevention Mechanisms (CPM), Legal Infrastructure Assessment Model (LIAM), and conflict resolution further illustrates that technology alone is insufficient to achieve higher legal effectiveness. Rather, legal effectiveness arises from the combination of legally binding enforcement instruments and IT tools. Accordingly, this study provides limited support for the adaptive governance models identified in previous cybersecurity research [9], but diverges from these models insofar as flexible use of IT, in the absence of accompanying legally binding provisions, generates at best moderate improvements in effectiveness.

On the other hand, the UN Global Counter-Terrorism Strategy provides an example of the constraints imposed by universally applicable legal frameworks that rely on political mediation. Even though IT incorporation resulted in a shorter time-to-conflict resolution and a lower number of norm violations, substantial ambiguities persisted regarding procedural accountability and real-time enforceability. The findings of this study provide support for previous studies in the literature indicating that global security instruments frequently prioritize inter-state consensus building over the potential of the security instrument to operate effectively in practice. Unlike previous studies, which were descriptive in nature, this study provides evidence for how ambiguities in international law can restrict the capability of digital tools to utilize their full potential in international security governance.

The OSCE framework provides an intermediate case. Although the OSCE framework is not legally binding, IT incorporation provided quantifiable

gains in transparency and norm compliance. The findings of this study contradict the common assumption that soft-law instruments are inherently ineffectual. Nevertheless, this study finds that the variability of effects of voluntary mechanisms for implementing soft-law instruments is particularly pronounced concerning cross-border surveillance and data sharing. Even though OSCE recommendations facilitate normative convergence, they are not capable of replacing legally binding obligations where advanced digital enforcement tools are utilized.

A key contribution of this study is its examination of the relationship between artificial intelligence (AI)-enabled legal decision-making and surveillance tools. The vast majority of previous research examined the ethics of AI-enabled tools (misinformation; public distrust, etc.) [16 – 17], without examining the impact of AI-enabled tools on the law. This study builds upon prior studies in demonstrating that AI-enabled tools may be used to enhance legal effectiveness and legal transparency if the tools are implemented with legally enforceable procedural safeguards and audit mechanisms. On the other hand, without such safeguards, the use of AI-enabled tools could increase jurisdictional dispute and rights violation as opposed to decreasing them.

Finally, the results from this study identified significant limitations and contradictions in the relationship between IT integration and legal compliance. Specifically, while there were fewer violations of norms among all jurisdictions examined after IT was integrated, the data also demonstrated that in some cases, the degree of violation increased; thus, the relationship is not always positive. However, on the other hand, IT integration simultaneously created new vulnerabilities (e.g., systemic biases, autonomous overreaching, and technological disparities among states) by increasing dependency on the availability of data, the interoperability of systems, and the accuracy of algorithms.

Like many studies that view digitalization as a linear progression, this study recognizes that digitalization plays two roles simultaneously - as both a facilitator and a constraint for international law.

Finally, this study utilizes a comparative methodology to examine the impact of IT on institutional performance across multiple international security regimes. Unlike previous sector-specific assessments (labour law [13]; e-government [14]; and health data protection [15]), this study examines the broadened influence of IT

on institutional performance utilizing an international legal lens at the macro-level. Through utilization of a comparative modeling methodology, this study identifies structural patterns that remain opaque in single-sector studies.

Additionally, this study critically assesses its own methodological assumptions. While simulation-based legal modeling permits controlled comparison, it fails to fully represent the wide scope of political contingency and informal practices that influence international cooperation in practice. This study builds upon prior studies in demonstrating that AI-enabled tools may be used to enhance legal effectiveness and legal transparency if the tools are implemented with legally enforceable procedural safeguards and audit mechanisms. On the other hand, without such safeguards, the use of AI-enabled tools could increase jurisdictional dispute and rights violation as opposed to decreasing them.

Finally, the results from this study identified significant limitations and contradictions in the relationship between IT integration and legal compliance. Specifically, while there were fewer violations of norms among all jurisdictions examined after IT was integrated, the data also demonstrated that in some cases, the degree of violation increased; thus, the relationship is not always positive. Harmonizing standards, establishing mechanisms for accountability and legally mandating transparency requirements will therefore constitute the main components of long term sustainable digital security governance.

## 6. LIMITATIONS

1. Limited harmonization of international legal norms. Despite the growing importance of information technologies, the lack of unified international legal standards complicates effective cross-border cooperation in the field of ensuring public security. Such fragmentation of the regulatory field reduces the level of legal certainty necessary for the integration of digital tools into security systems.

2. Rapid obsolescence of technologies. The pace of technological development significantly exceeds the speed of updating legislation. As a result, regulatory acts quickly lose their relevance. Such a time gap limits the ability of legal systems to respond promptly to new digital threats.

3. Data sovereignty and jurisdictional conflicts. The growing trend towards the introduction of national restrictions on data flows and cloud services leads to the emergence of jurisdictional

conflicts. Such barriers complicate the implementation of international IT solutions focused on the security sector and hinder the coordination of actions of law enforcement agencies of different states.

4. Limitations of empirical research. Insufficient access to secret or confidential government information complicated the empirical verification of the legal and technical models proposed in this study. This narrowed the possibilities for practical evaluation of the proposed solutions and limited the conduct of full-fledged comparative analytics.

## 7. RECOMMENDATIONS

1. Developing uniform international legal instruments. States should support the creation of binding international treaties or model laws that clearly regulate the IT use to ensure public safety and maintain law and order. Unified definitions and procedures will facilitate effective transnational cooperation.

2. Implementing adaptive regulatory mechanisms. Legal systems should implement flexible legislative approaches, including regulatory sandboxes and technology-neutral norms. This will enable taking into account the rapid pace of development of digital tools and ensure the sustainability of legal regulation.

3. Promoting cross-border data management agreements. International organizations should intensify the conclusion of multilateral agreements that guarantee lawful, secure and interoperable data exchange. A clear definition of jurisdictional rules will help to overcome the fragmentation of the legal space and support the development of a global security infrastructure.

4. Strengthening interdisciplinary research and transparency. Further research should integrate technical, legal, and ethical considerations, engaging a broad range of stakeholders, including civil society and cybersecurity experts. The introduction of declassification and anonymization protocols will help expand access to critical empirical data.

## 8. DIFFERENCE FROM PRIOR RESEARCH AND SCIENTIFIC CONTRIBUTION

This study is different from other studies in several ways. It is based upon a new theoretical model which includes a comparative and empirical examination of how technology shapes international public safety regulations in different models of governance. First, whereas most studies of

information technology have examined a single technology — for example, AI surveillance, cybersecurity platforms or blockchain systems — this study examines all three technologies together using a comprehensive legal/technological assessment model.

Using Legal Modelling of Standards (LMS) — a method used to model legal standards — the study also uses doctrinal comparative analysis — an analytical methodology — and the Legal Impact Assessment Method (LIAM) — a method used to assess the impact of laws — to provide a structured framework to measure legal compliance, efficiency and transparency as interrelated effects of integrating IT into public safety regulation. This multidimensional approach represents a significant improvement over qualitative assessments and allows for the first time systematic comparisons between international legal regimes to be made.

Second, while many studies of information technology have identified ethical problems, provided policy recommendations, or documented technical risks associated with digitalization, none have evaluated their operational legal implications. In contrast, the findings of this study demonstrate how different legal architectures affect the efficacy of IT in public safety regulation. For example, the study finds that public safety organizations operating in jurisdictions where there are binding and enforceable legal frameworks (e.g., Europol) experience significantly greater benefits from digitalization than organizations operating in jurisdictions with politically-coordinated or soft-law regimes. These findings challenge the widespread assumption that the level of technological sophistication is the primary determinant of regulatory success.

Third, this study represents a methodological advancement because it operationalizes international legal norms in a simulated laboratory environment. Using the Lex Sim-Lab platform, the study simulates legal conflict resolution, procedural protections and cross-border enforcement issues that are difficult to identify empirically due to the confidential nature of the issues or restrictions related to national security or political sensitivities. As such, this research contributes to the development of a replicable research tool for studying international legal performance in digital security contexts.

Fourth, this study advances the growing body of literature about artificial intelligence in public safety by moving away from focusing solely on abstract risks and towards analyzing the

institutional legal design. While many early studies of AI emphasized disinformation, bias and distrust deficits, this study finds that AI can improve the efficiency and transparency of legal regulation if it is incorporated into enforceable accountability structures. At the same time, this study finds that institutions lacking strong legal design increase the risk of harm associated with algorithmic governance.

Fifth, the primary scientific contribution of this research is its reconceptualization of information technology as a legal "stress-test" and not simply as a neutral tool. Through its empirical demonstration of how digital technologies reveal structural weaknesses in international legal regulation — particularly in relation to jurisdiction, data sovereignty, and procedural accountability — the study identifies new knowledge on how international law must evolve to continue to function effectively in the digital age.

Together, these contributions establish the article as a theoretically-based and methodologically innovative study that builds upon our understanding of international legal regulation of public safety under conditions of rapid digital change.

## 9. CONCLUSIONS

"The study stated that "Information Technology is not merely an added instrument of international legal regulation of public safety, law and order; but has the potential of becoming a decisive element in the efficiency of the regulatory process."

Using a comparative legal-technical analysis of international security frameworks (the comparison was made using the security frameworks of the United States, European Union and China), the study identified that the extent of the influence of digitalization in the field of security is primarily dependent upon the legal regulations governing the use of technological tools, and not by the degree of technological progress achieved.

Thus, the conclusions drawn by the study were consistent with the fact that regulatory models having a legally binding and institutionally established character result in significantly greater benefits from the integration of IT, compared to those models which rely on political coordination or voluntary compliance. For example, the regulatory model employed by Europol demonstrates how the presence of enforceable mandates, standardized procedures, legally established accountability mechanisms, and other characteristics of a legal regime can convert digital technologies into tools for enhancing compliance, transparency and cross-

border coordination amongst agencies. On the contrary, global and consultative models produce less favorable results due to the same reasons, and additionally, create serious issues with regard to jurisdictional ambiguity, procedural accountability and data sovereignty.

Therefore, the article contributes substantially to science through the establishment of an analytically replicable framework that combines legal modeling, comparative doctrinal analysis and impact assessment to evaluate international legal performance at times when there are rapid technological developments. In contrast to all previously conducted studies that were either descriptive/policy-oriented, this study establishes empirical relationships between the integration of information technologies and measurable legal effects (i.e., compliance with norms, transparency of procedural decisions, and the efficiency of conflict resolution).

In addition to presenting new knowledge concerning how international law accepts (and does not accept) digital enforcement tools in the form of emerging technologies, the results of the study present new insights into how artificial intelligence and automated decision-making systems may increase public safety governance only if they are embedded in legally enforceable safeguards. If no regulatory framework is established, the digital tools may continue to fragment the law as it presently exists, and thus potentially infringe upon fundamental rights. Therefore, this research creates new knowledge related to the ongoing discussion regarding the regulation of digital technologies, and shifts the focus away from the risks associated with specific technological applications, toward the institutional/legal environment that is required for the creation of responsible and efficient digital governance.

Finally, the study will develop empirically-based policy recommendations that will enable international organization and decision-makers to better guide their future activities. Specifically, the study emphasizes the need to prioritize the harmonization of legal standards, enforceable mechanisms for transparency, and procedural accountability in the design of digital security systems. The study's results are directly applicable to the development of international treaties, regulatory instruments, and technical standards to respond to cross-border public safety challenges. In general, the study represents new insights into the evolution of the relationship between information technologies and international legal regulation, by transforming digitalization into a test

of the resiliency of international law, instead of viewing it as a self-sufficient solution. Therefore, the study will represent the foundation for future interdisciplinary research regarding the governance of artificial intelligence, big data, and digital surveillance in international security contexts, and underscores the necessity for international law to adjust to technological innovations, while retaining basic legal principles.

#### REFERENCES:

- [1] Ontario Human Rights Commission. Policy on Eliminating Racial Profiling in Law Enforcement, 2023. URL: <https://www3.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement> [accessed: 25.10.2025].
- [2] I. Popovich, A. Rusetskyi, E. Nazymko, M. Korniienko & A. Polianskyi, "Peculiarities of Law Enforcement System Functioning in the Context of Digitalization," *Edelweiss Applied Science and Technology*, Vol. 8, No. 4, 2024, pp. 2348–2355. <https://doi.org/10.55214/25768484.v8i4.1603>
- [3] V. Komarnytskyi, T. Arifkhodzhaieva, O. Oderii & V. Kovalenko, "International Security: Current Situation and Ways of Improvement Legal Regulation", *Jurnal Cita Hukum*, Vol. 9, No. 3, 2021, pp. 539–550. <https://doi.org/10.15408/jch.v9i3.22653>
- [4] V. Artemov, Y. Ishchenko, A. Rusnak, V. Trepak & M. Denysenko, "The Role of American Intelligence in Shaping Foreign Policy Strategies", *Edelweiss Applied Science and Technology*, Vol. 8, No. 5, 2024, pp. 1385–1399. <https://doi.org/10.55214/25768484.v8i5.1842>
- [5] N. Lytvyn, H. Andrushchenko, Y. Zozulya, O. Nikanorova & L. Rusal, "Enforcement of Court Decisions as a Social Guarantee of Protection of Citizens Rights and Freedoms", *Prawo i Więź*, Vol. 39, No. 1, 2022, pp. 80–102. <https://doi.org/10.36128/prw.vi39.351>.
- [6] Centre for European Policy Studies. Online Content Regulation: Towards a Principled Approach, 2022. URL: [https://cdn.ceps.eu/wp-content/uploads/2022/10/CEPS-Task-Force-Report\\_Online-Content-Regulation.pdf](https://cdn.ceps.eu/wp-content/uploads/2022/10/CEPS-Task-Force-Report_Online-Content-Regulation.pdf) [accessed: 25.10.2025].
- [7] United Nations Office of Counter-Terrorism. Establishing a Legislative Framework for the Use of New and Emerging Technologies in Counter-Terrorism, 2023. URL: [https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoc\\_t\\_establishing\\_legislative\\_framework\\_web.pdf](https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoc_t_establishing_legislative_framework_web.pdf) [accessed: 25.10.2025].
- [8] O. Sydoruk, V. Bashtannyk, F. Terkhanov, O. Kravtsov, L. Akimova & O. Akimov, "Integrating Digitization into Public Administration: Impact on National Security and the Economy through Spatial Planning", *Edelweiss Applied Science and Technology*, Vol. 8, No. 5, 2024, pp. 747–759. <https://doi.org/10.55214/25768484.v8i5.1740>
- [9] O. Akimov, M. Karpa, O. Parkhomenko-Kutsevil, V. Kupriichuk & A. Omarov, "Entrepreneurship Education of the Formation of the E-commerce Managers Professional Qualities", *International Journal of Entrepreneurship*, Vol. 25, No. 7, 2021.
- [10] H. M. Melaku, "A Dynamic and Adaptive Cybersecurity Governance Framework", *Journal of Cybersecurity and Privacy*, Vol. 3, No. 3, 2023, pp. 327–350. <https://doi.org/10.3390/jcp3030017>
- [11] R. Sidharta & P. E. T. Dewi, "The Role of Cyber Notary in the Field of Digital International Trade in Indonesia", *Notariil Jurnal Kenotariatan*, Vol. 8, No. 1, 2023, pp. 1–7. <https://doi.org/10.22225/jn.8.1.2023.1-7>
- [12] O. Kostenko & V. Mangora, "Areas of Development of Legal Regulation of Identification Data Management", *Information and Law*, Vol. 1, No. 40, 2022, pp. 54–60. [https://doi.org/10.37750/2616-6798.2022.1\(40\).254342](https://doi.org/10.37750/2616-6798.2022.1(40).254342)
- [13] S. Shabanova & A. Lazebna, "Information Security of Labor Law Subjects", *The Journal of V N Karazin Kharkiv National University Series Law*, Vol. 32, 2021, pp. 15–20. <https://doi.org/10.26565/2075-1834-2021-32-02>
- [14] N. M. A. Raza, "Cyber Security and Data Privacy in the Era of E-Governance", *Social Science Journal for Advanced Research*, Vol. 4, No. 1, 2024, pp. 5–9. <https://doi.org/10.54741/ssjar.4.1.2>
- [15] J. Espinoza, A. T. Sikder, J. Dickhoner & T. Lee, "Assessing Health Data Security Risks in Global Health Partnerships: Development of a Conceptual Framework", *JMIR Formative Research*, Vol. 5, No. 12, 2021, e25833. <https://doi.org/10.2196/25833>
- [16] D. Guo, H. Chen, R. Wu & Y. Wang, "AIGC Challenges and Opportunities Related to Public Safety: A Case Study of ChatGPT", *Journal of Safety Science and Resilience*, Vol. 4, No. 4,

- 2023, pp. 329–339. <https://doi.org/10.1016/j.jnlssr.2023.08.001>
- [17] P. Robles & D. J. Mallinson, “Artificial Intelligence Technology, Public Trust, and Effective Governance”, *Review of Policy Research*, Vol. 42, No. 1, 2023, pp. 11-28. <https://doi.org/10.1111/ropr.12555>
- [18] R. Bianda, A. Gunaepi & M. M. Munir, „Offering Sharia Securities through Technology Based Crowdfunding Services Based on Sharia Principles According to MUI Fatwa”, *Journal of World Science*, Vol. 2, No. 3, 2023, pp. 332–340. <https://doi.org/10.58344/jws.v2i3.240>
- [19] S. T. Alvi, M. N. Uddin, L. Islam & S. Ahamed, “DVTChain: A Blockchain-Based Decentralized Mechanism to Ensure the Security of Digital Voting System”, *Journal of King Saud University - Computer and Information Sciences*, Vol. 34, No. 9, 2022, pp. 6855–6871. <https://doi.org/10.1016/j.jksuci.2022.06.014>
- [20] MiniTAB. Data Analysis, Statistical & Process Improvement Tools, 2025. URL: <https://www.minitab.com/en-us/> [accessed: 25.10.2025].
- [21] M. Usiagwu, “Cross-Border Data Compliance: Navigating Public Security Regulations in a Connected World”, *Tripwire State of Security*, 2025. URL: [https://www.tripwire.com/state-of-security/cross-border-data-compliance-navigating-public-security-regulations-connected?utm\\_source=chatgpt.com](https://www.tripwire.com/state-of-security/cross-border-data-compliance-navigating-public-security-regulations-connected?utm_source=chatgpt.com) [accessed: 25.10.2025].
- [22] O. Roberts, “What to Expect in 2025: AI Legal Tech and Regulation (65 Expert Predictions)”, *National Law Review*, 2024. URL: <https://natlawreview.com/article/what-expect-2025-ai-legal-tech-and-regulation-65-expert-predictions?utm> [accessed: 25.10.2025].
- [23] J. Rowe, N. Sun, R. Wilkinson, Y. Afina & M. Buchser, “Towards a Global Approach to Digital Platform Regulation: 02 Global Regulatory Trends” [Research Report]. Chatham House & Global Partners Digital, 2024. URL: <https://www.chathamhouse.org/2024/01/towards-global-approach-digital-platform-regulation/02-global-regulatory-trends?utm> [accessed: 25.10.2025].
- [24] Europol. Common Challenges in Cybercrime 2024. Europol, 2024. URL: [https://www.europol.europa.eu/cms/sites/default/files/documents/Common\\_Challenges\\_in\\_Cybercrime\\_2024.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf) [accessed: 25.10.2025].
- [25] Europol. Common Challenges in Cybercrime Investigations: 2024 Update. European Union Agency for Law Enforcement Cooperation, 2024. URL: [https://www.europol.europa.eu/cms/sites/default/files/documents/Common\\_Challenges\\_in\\_Cybercrime\\_2024.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf) [accessed: 25.10.2025].
- [26] Europol. Programming Document 2025–2027, 2024. URL: [https://ipex.eu/IPEXL-WEB/download/file/8a8629a8945e0af901945f53994e001a/Europol\\_Programming\\_Document\\_2025-2027.pdf](https://ipex.eu/IPEXL-WEB/download/file/8a8629a8945e0af901945f53994e001a/Europol_Programming_Document_2025-2027.pdf) [accessed: 25.10.2025].
- [27] European Commission. Cooperation with Europol, 2025. URL: [https://home-affairs.ec.europa.eu/policies/internal-security/law-enforcement-cooperation/cooperation-europol\\_en](https://home-affairs.ec.europa.eu/policies/internal-security/law-enforcement-cooperation/cooperation-europol_en) [accessed: 25.10.2025].
- [28] OSCE. (2023). Ensuring Human Rights Compliance in Cybercrime Investigations: A Guide for Law Enforcement and Criminal Justice Authorities, 2023. URL: <https://www.osce.org/files/f/documents/e/3/554901.pdf> [accessed: 25.10.2025].
- [29] United Nations. Enhancing Law Enforcement Capabilities in Countering Terrorism. United Nations Office of Counter-Terrorism (UNOCT), 2021. URL: [https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct\\_law\\_enforcement\\_capabilities\\_web2.pdf](https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_law_enforcement_capabilities_web2.pdf) [accessed: 25.10.2025].
- [30] United Nations Department of Economic and Social Affairs. E-Government Survey 2024: Governing through Digital Technologies (Web Version). United Nations, 2024. URL: <https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf> [accessed: 25.10.2025].
- [31] Secretariat International. Global Financial and Economic Crime Outlook 2025, 2025. URL: <https://secretariat-intl.com/wp-content/uploads/2025/04/Secretariat-Global-Financial-and-Economic-Crime-Outlook-2025.pdf> [accessed: 25.10.2025].
- [32] Organization for Security and Co-operation in Europe. Best Practice Guide: Strengthening Anti-Corruption Frameworks with Digital Tools. OSCE, 2022. URL: [https://www.osce.org/files/f/documents/7/d/518247\\_0.pdf](https://www.osce.org/files/f/documents/7/d/518247_0.pdf) [accessed: 25.10.2025].
- [33] Europol. SIRIUS Digital Evidence Situation Report 2022. European Union Agency for Law

- Enforcement Cooperation, 2022. URL: [https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS\\_DESR\\_2022.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_DESR_2022.pdf) [accessed: 25.10.2025].
- [34] United Nations. UNOCT Annual Report 2024. United Nations Office of Counter-Terrorism, 2024. URL: [https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct\\_2024\\_annual\\_report\\_eng.pdf](https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_2024_annual_report_eng.pdf) [accessed: 25.10.2025].
- [35] Organization for Security and Co-operation in Europe (OSCE). Countering Terrorism, 2025. URL: <https://www.osce.org/countering-terrorism> [accessed: 25.10.2025].
- [36] Organization for Security and Co-operation in Europe (OSCE). Legal and Policy Framework for Combating Cybercrime in the OSCE Region, 2025. URL: [https://www.osce.org/files/f/documents/3/5/107686\\_2.pdf](https://www.osce.org/files/f/documents/3/5/107686_2.pdf) [accessed: 25.10.2025].
- [37] Europol. Data Protection and Transparency, 2025. URL: <https://www.europol.europa.eu/about-europol/data-protection-transparency> [accessed: 25.10.2025].
- [38] United Nations Office of Counter-Terrorism. UNOCT Strategic Plan Results Framework 2022–2025, 2022. URL: [https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct\\_strategic\\_plan\\_results\\_framework\\_2022-25.pdf](https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_strategic_plan_results_framework_2022-25.pdf) [accessed: 25.10.2025].
- [39] OSCE/ODIHR. Republic of Albania Parliamentary Elections, 23 June 2013: Final Report. Organization for Security and Co-operation in Europe, 2025. URL: <https://www.osce.org/files/f/documents/f/2/180731.pdf> [accessed: 25.10.2025].
- [40] United Nations. UN Global Counter-Terrorism Strategy, 2025. URL: <https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy> [accessed: 25.10.2025].
- [41] European Data Protection Supervisor. Annual Report 2024: Acting for the Future of Data Protection (PDF). Brussels: European Data Protection Supervisor, 2025. URL: [https://www.edps.europa.eu/system/files/2025-04/edps\\_annual\\_report-2024\\_en.pdf](https://www.edps.europa.eu/system/files/2025-04/edps_annual_report-2024_en.pdf) [accessed: 25.10.2025].