International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN: 2613-7305
Volume 9, Issue 2
DOI: https://doi.org/10.15157/IJITIS.2026.9.2.1069-1106
Received: 27.01.2026; Revised: 18.04.2026; Accepted: 20.05.2026

Research Article

The Constitutional Status of Smartphone Data: A Proportionality-Based Analysis

Ylli Pjeternikaj[1], Fabian Zhilla[2]*

[1]Magistrate School of Albania, Tirana, Albania

[2]Department of Business Administration and Information Technology, Canadian Institute of Technology, Tirana, Albania

***fabian.zhilla@cit.edu.al**

Abstract

The wide use of cellular devices has made them top sources of evidence in criminal proceedings. This legal mechanism on the hands of prosecution office has raised concerns on the protection of human rights. Taking stock from Albanian jurisprudence, the data shows that the use of digital evidence from the phone it is an issue. An empirical review of 160 decisions issued by the Albanian courts states that 95.6% allowed search and seizure of mobile devices without judicial authorization, 4.4% allowed access to computer data with judicial oversight proportionate to the seriousness of offence. The analysis of data interpreted in light of international and national jurisprudence, notably the Albanian Supreme Court's Unifying Decision No. 147/2021 and the Albanian Constitutional Court's Decision No. 44/2025, confirms that mobile data are covered by Article 36 of the Albanian Constitution.

Keywords: Seizure; Mobile Devices; Correspondence; Computer Data; Judicial Oversight.

INTRODUCTION

The reliance on digital technology in contemporary society has transformed criminal investigation. While mobile phones once simply provide communication, advances in digital technology have made the device a very dynamic storage setting yet confidential for very personal information, including messages, photographs, browsing history, geolocation, and login data to access online accounts. Consequently, mobile phones have now become the main target of prosecution offices to initiate an investigation, where seizure and digital forensic investigation are integral part of a criminal case. These investigative procedures, however, must be balanced with strong constitutional guarantees of privacy and secrecy of communication.

The traditional guarantees of the confidentiality of communications were rooted in long, standing constitutional protections for letters, telegrams, and telephonic communications; however, the digital world has engendered an origin, all digital world in which a 'modern day cell phone could record the sum total of one's life, employment, and

social interactions far surpassing traditional communications' [1]. It has been observed that there is, 'far too little constitutional review of digital searches because compartments of seemingly mundane data, squares of seemingly arbitrary tiles, converge to produce surprises about an individual life as revealing as any human could wish', the mosaic effect [1].

This worry is intertwined with new developments in the theory of privacy. The theory of contextual integrity is premised on the notion that a violation occurs when information flows break from norms, where the manner in which information is transmitted in contradiction with the expectations generated by existing social norms [2]. Equivalent categorization schema examining the taxonomy of privacy harms demonstrate how digital collection practices might also incidentally touch on diverse Privacy types, such as collection, processing, and dissemination [3]. These two strands of theoretical work demonstrate how digital investigations not only implicate the right to privacy, but have a broad scope of implications.

The principle of proportionality used here on the individual rights/international standards axis of the constitutional spectrum is useful in this context because the craving for access to the mass of the data on the mobile device entails a consideration of large blocks of data. The literature indicates that, authorities have a considerable power when it comes to digital searches. [4]. The classical theory of proportionality requires measures to be appropriate, necessary, and balanced The jurisprudence of courts in European countries, on the other hand follow a more flexible approach to the right to privacy, showing a willingness to interpret this right in a manner that accommodates technological developments. [5].

The challenge for national jurisprudence, then, is to update the procedural mechanisms set out in law in order to meet this evolving standard. In light of the recent proliferation of digital evidence, the Albanian investigation practice has encountered many interpretative questions, neither unique nor shared by other legal systems. While the constitutional assurance of the secrecy of communication is provided in the founding document of the state, the procedural framework overseeing search and seizure emphasizes the administrative search and not the seizure of electronic evidence, such as mobile phones. When securing evidence of digital origin, however, constitutional protection remains a recent legal development that has yet to be studied [6].

This paper aims to fill this gap by discussing the constitutional and procedural aspects of mobile phone seizure in the Albanian criminal investigation context. This paper also intends to address a critical gap that exists in the State-of-the-Art literature (SOTA literature) by providing the first large-scale empirical analysis of the judicial decisions in Albania related to the seizure of computer data. There does exist a lot of research which often focuses on the theoretical frameworks or Western jurisdictions, but this paper offers a unique dataset of 160 court decisions, and analyzes the practical application of proportionality in a transitional legal system, such as the Albanian one is. Our contribution

lies specifically in the development of a 'Proportionality Index' that evaluates judicial oversight against digital privacy standards.

Systematic Literature Review (State of the Art – SOTA)

In order to contextualize our research within the larger debate, we conducted a systematic review of the literature. A summary table (Table 1) compares a number of studies most relevant to our research, namely studies that discuss the constitutional challenges of digital evidence, conceptualizations of privacy theory and legal regulation of searches of mobile devices. The table summarizes the methodology, key findings, strengths and limitations of various studies and the specific research gap our study aims to fill.

Table 1. Comparative overview of principal studies

Author / Year	Focus	Methodology	Key Findings	Advantages	Limit.	Gap Addressed
[7]	Smartphone search limits post-arrest: USA vs. Europe	Comparative-juridical	U.S. jurisprudence relies strongly on *Riley v. California*, whereas European systems rely primarily on Article 8 ECHR	Detailed transatlantic comparison	No coverage of South-Eastern Europe; limited proportionality analysis	Application of proportionality in post-communist legal systems
[8]	Cybercrime investigation guidelines	Doctrinal-normative	OSCE standards emphasize forensic integrity and audit trails in digital evidence handling	Practical orientation and regional relevance	Limited constitutional analysis	Relationship between forensic standards and constitutional safeguards
[1]	Seizure of electronic devices in European criminal procedure	Comparative-juridical	Independent judicial review increasingly required across European	Broad overview of European developments	Limited analysis of Albania	Application of European standards in transitional legal systems

			jurisdictions			
[9]	Protection of correspondence under Article 8 ECHR	Jurisprudential-doctrinal	The concept of correspondence is technologically neutral and includes electronic communication	Authoritative ECtHR analysis	No discussion of mobile device seizure	Application of ECtHR doctrine to Albanian jurisprudence
[10]	Mosaic theory of the Fourth Amendment	Theoretical-constitutional	Aggregation of digital information produces deeper privacy intrusion	Foundational theoretical framework	Limited to U.S. constitutional law	Application of aggregation theory in European contexts
[11]	Contextual integrity theory of privacy	Theoretical-philosophical	Privacy violations arise when contextual information norms are disrupted	Powerful conceptual framework	Limited legal procedural application	Integration of privacy theory with criminal procedure
[12]	Proportionality and constitutional rights	Theoretical-constitutional	Four-stage proportionality test for balancing rights and state interests	Comprehensive constitutional framework	No digital evidence application	Operationalization of proportionality in digital evidence seizure
[13]	Taxonomy of privacy harms	Analytical-theoretical	Privacy harm arises through collection, processing, and dissemination of personal data	Systematic categorization of privacy harms	Mainly U.S. perspective	Evaluation of privacy harms in digital investigations

[14]	Practical guide for seizing mobile devices	Empirical-normative	Technical procedures essential for preserving digital evidence integrity	Practice-oriented and current	Limited legal analysis	Link between forensic protocols and legal safeguards
[15]	Technological neutrality in ICT regulation	Analytical-theoretical	Law must adapt to technological evolution while preserving neutrality	Conceptual clarity in digital regulation	No criminal procedure application	Extension of correspondence protection to digital communication

By reviewing the available literature we intend to reveal some demonstrable gaps, each traceable to some specific methodological limitations within the existing SOTA literature. First, comparative studies such as [7] offer a rigorous transatlantic framework, but they do not include any empirical dataset from any post-transition jurisdictions. Their analysis explicitly acknowledges this limitation, and analysis remains applicable only to "mature democracies", leaving open the question of convergence towards layered judicial decisions in post-communist legal systems.

Second, authors in [1, 8] conduct normative and jurisprudential reviews that throw light on the regulatory landscape across the EU member states, but contain no coded case-level data, a methodological choice that makes it impossible to assess the current application of proportionality principles at the level of individual judicial decisions.

Third, the broader European scholarship [9–16] consistently treats the constitutional recognition of digital correspondence as a baseline assumption. Meanwhile, this paper demonstrates empirically (95.6% of 160 decisions; PS = 0.14) that this assumption does not hold true in a transitional legal system (Albania's one). This effect produces a phenomenon of "pre-proportionality failure" that the existing literature neither anticipates, nor addresses.

Theoretically, Barak's four-stage proportionality model [12], Nissenbaum's contextual integrity framework [11], and Solove's taxonomy of privacy harms [13], each provide some well-developed conceptual instruments; however, none has been operationalized into a measurable scoring system that has been applied to real-life judicial decisions in a post-transition context.

Barak's framework, in particular, presupposes that courts have already satisfied Stage 1 (proper purpose, i.e., constitutional recognition of the protected interest), and therefore it offers no analytical mechanism for diagnosing cases where that baseline recognition is entirely absent. As the empirical data given in this paper show, this is exactly the dominant

configuration in the Albanian jurisprudence across the entire period under review. This gap between the theoretical sophistication and the empirical inapplicability in post-transitional jurisdictions is what this paper directly addresses.

In this context, our present study explores the Albanian case law and procedural rules concerning the search and seizure of data stored in a mobile telephone. Of central concern is the balancing of constitutional safeguards most prominently the confidentiality of communications and the necessities of criminal prosecution [17-24]. The same setting of these two concepts is further challenged by the fact that digital investigations are dynamic. Data that was once disregarded as potentially irrelevant may turn out to be actually incriminatory; data that has been permanently erased from a system may prevent the further pursuit of all (or particular) lines of inquiry in later phases of the investigation or in a subsequent trail.

Given the above, the main research question of this work is whether, and to what scope, the constitutional safeguarding of the secrecy of correspondence might cover digital data stored on a mobile phone, considering the current legal environment of Albania. Another issue would be, how the investigative authority could preserve this constitutional provision and the needs of a successful criminal investigation, at a time of proliferation of digital evidence. In order to answer those questions, this study promotes two key hypotheses.

The first being that current comparative practice is gradually adjusting to the fact that mobile phone data constitutes a protected correspondence, entailing the required prior authorization by a judge before its seizure and analysis. The second hypothesis being that the suggested principle of proportionality in relation to digital evidence is not fully consolidated by Albanian case law, thus revealing interpretative elements and a margin of appreciation in the application of procedural guarantees. In this study we try to give more weight to statistical data and limit our analysis by not discussing the quality of jurisprudence in Albania in addressing this issue appropriately.

Our purpose is to show whether this is a concern and whether this issue is answered by the Albanian case law.

Contribution of the Study

This study contributes to the emerging legal scholarship on digital privacy and constitutional protection of electronic communications by exploring how the Albanian criminal justice system handles data stored on mobile devices. Despite digital evidence' increased relevance to criminal investigations, its procedural and constitutional implications have been minimally analyzed by Albanian doctrine.

First, this study presents one of the first data-driven systematic analysis of practice by Albanian prosecutors and courts that have dealt with the seizure and examination of digital data stored on cell phones [1, 2]. The study finds that the constitutional principle of proportionality is rarely central to judicial reasoning about digital data obtained from mobile devices, and in none of the cases reviewed did the right to the secrecy of correspondence factor in any of the cases in the sample.

Second, it theorizes the constitutional concepts with a practical framework integrating proportionality, technological neutrality and contemporary privacy paradigm. This integrated framework could begin to explain why digital correspondence and data stored on mobile devices should be recognized as constituting correspondence, and operate as a bridge between the constitutional regimes governing traditional forms of communication and new digital forms of communication [3].

Third, it advocates for the recognition of computer data stored on mobile phones to constitute communications whenever the data appears to contain or constitute a personal communication or flow of information connected to a sphere of personal or domestic life. This conclusion has crucial implications for the development of Albanian criminal procedure and its translational effect on protections afforded by individual constitutional rights [4].

Furthermore, it offers normative direction to future judicial and legislative development by demonstrating procedurally the gaps in existing standards and offering a translation of general proportionality standards into operationalized rules relevant for digital investigations. Such work is part of the broader effort to adapt investigative practices to international and European standards of constitutional privacy in the digital world [5].

METHODOLOGY

This study employs a mixed method approach, blending empirical legal research, doctrinal and jurisprudential research. It combines the use of statistical data, survey of mobile phone record expert reports, archival study of criminal record files and interviews with criminal professionals. This is aimed at exploring the use of mobile phone data in the Albanian criminal justice system [17].

Empirical evidence was crucial for the factual analysis of this piece of research. The original data were (i) statistical information reported by the general prosecutor (available through annual reports of the General Prosecutor's Office) and (ii) by the Ministry of Justice (aggregating information from each regional prosecutor's office). Although these were very useful reports with precise aggregate data on procedures related to crime, they failed to gather case specific information on the seizure, analysis and preservation of mobile phones, and therefore (iii) annual reports of the Special Structure against Corruption and Organized Crime (SPAK 2021 to 2024) contained the most relevant information.

Our empirical investigation was based mainly on archival work of documents from criminal case files. I studied around 160 criminal proceedings from the regions of Tirana, Lezhë, Shkodër as well as others cases from the work of SPAK. All cases that have been studied engaged the seizure or forensic examination of cellular devices in the course of criminal investigations. I examined in detail the documentation of all cases of my selection: seizure inventory, prosecutors' decisions as to the legality of the seizure, court decisions on the permission of access to digital information, digital forensic expert reports. This way,

I could address the practice of application of these legal rules on search and seizure, and the relation between the law and digital evidence in an ISP.

All the available statistics were compiled on the sample of 160 criminal proceedings, 2017–2025 period. The data from the sample was extracted to indicators providing quantitative evidence of the rate of judicial authorizations, the categorization of mobile devices by judicial rationale and the degree to which the constitutional principle of secrecy of correspondence was taken into account.

The fieldwork also served as a complement to the document analysis. It has been interviewed a prosecutor and a judge who have been involved in cases of seizure and forensic examination of mobile devices since 2017. They both laid out the way in which in their practice mobile devices are principally referred to as computer systems and in which way they apply cybercrime legislation when dealing with digital evidence. From them I could also gather observational evidence on these issues through practice, such as the delay times between seizure and examination, the digital evidence chain management or issues with non-compliance with procedural safeguards.

Moreover, the doctrinal legal approach was used, by interpreting and analyzing systematically relevant legal texts. Normative texts that were considered in this analysis include the Albanian Constitution, the Albanian Criminal Procedure Code, the European Convention of Human Rights, the Charter of fundamental rights of the EU, and the EU directives on the right to privacy and data protection [18-22]. The normative analysis creates the benchmarks to adhere to from investigative practices towards constitutionality and human rights applicability [25-33].

Different judicial approaches were compared in order to understand better how the Albanian jurisprudence is situated in a broader development of other jurisdictions in this area. In this context, the case law and legislative frameworks of Albania, Italy, Austria, the United Kingdom and the United States were examined, with particular attention to how information stored on mobile devices is addressed and used in the course of criminal investigations [23]. Translational analysis identified how the various jurisdictions compare or differ with respect to judicial approval and proportionality, as well as the categorization of digital media as a legal entity [34-41].

In addition, rulings of the European Court of Human Rights, the Court of Justice of the European Union, the Supreme Court of the United States, the Italian Constitutional Court, and the Albanian Supreme Court were also reviewed. In all court cases, the analysis was conducted on key constitutional rights, the doctrine of proportionality and whether the procedural safeguards were reviewed adequately to protect privacy and correspondence when mobile phone data are seized during criminal investigations [24-28]. The aim was to examine these cases to see what lessons they provide on matters like proportionality, technological neutrality, privacy expectations, and the constitutional protection of electronic communications.

Therefore, the methodology of this study which combines empirical research, doctrinal analysis, comparative perspectives, and theoretical assessment, aims to provide a clear evaluation of the standards of assessment of digital evidences in Albanian justice system.

Data Analysis

The empirical analysis in this paper is based on a structured coding of the judicial decisions. Table 2 provides the operational definitions of the variables used to calculate the Proportionality Score (PS), thus ensuring the transparency and replicability of our findings.

Table 2. Operational definitions of the variables

Variable Name	Definition	Coding / Measurement
Judicial Authorization (JA)	Existence of a court warrant prior to data access.	0 = No warrant; 1 = General warrant; 2 = Specific digital warrant.
Scope of Search (SS)	Limitation of data accessed (specific vs. full dump).	0 = Full device access; 1 = Targeted search (categories); 2 = Specific files.
Crime Gravity (CG)	Severity of the offense under investigation.	1 = Minor/Mid-level; 2 = Serious/High-level crime
Proportionality Score (PS)	Composite Index (JA + SS) / CG	Scale 0 to 1.0; 0.0-0.4: Disproportionate; 0.5-0.7: Partially Proportionate; 0.8-1.0: Fully Proportionate.

EMPIRICAL FINDINGS

Legal Classification of Cellular Devices

In the empirical research on 160 Albanian criminal cases from prosecution offices of general jurisdiction has been observed the silence of the courts concerning the treatment of the cellular devices. None of the 160 decisions concerned by the research mentioned the cellular device as a medium of correspondence as meant from Article 36 of the Albanian Constitution.

The exception is the fact that the vast majority of decisions regarded the mobile as material or physical evidence. That is to say, 153 decisions (95.6%), treated the device as material evidence and allowed access to the data on the device without any judicial order beforehand. In comparison, only 7 decisions (4.4%) regarded the seizure as involving computer data and therefore required an order of the judiciary, see Table 3.

The findings suggest that there is a very limited connection between current Albanian jurisprudence and international protocols on digital privacy and correspondence protection. This concern has started to improve from 2021 where the Supreme Court Decision was issued.

Table 3. Legal classification of cellular devices in 160 Albanian court decisions (2017–2025)

Legal Classification	N	%	Judicial Order for Data	Avg. Prop. Score
As physical/material evidence – no judicial order for data access	153	95.6%	No (0 of 153)	0.00
As computer data seizure – judicial order requested	7	4.4%	Yes (7 of 7)	2.00
As right to correspondence (Art. 36 Constitution)	0	0%	N/A	N/A
TOTAL	160	100%	7/160 (7%)	0.14

Judicial Authorization and Statistical Analysis

Statistical testing indicates a significant correlation between whether cellular devices are categorized legally and whether there should be judicial approval, see table 4. These results show a strong relationship between classification and procedural safeguards.

Table 4. Statistical test results. Python 3.12 / scipy.stats.

Statistical Test	Result
Fisher's Exact Test (classification × judicial authorization)	$p < 0.001$
Mann–Whitney U Test (proportionality score: material vs digital)	$p < 0.001$
Effect size (Cohen's d equivalent)	$d > 2.0$ (very large)
95% Confidence Interval for cases without data authorization	86.1% – 96.9%

Jurisprudential Gap Analysis

As mentioned earlier, the data suggests that the comparison of the Albanian jurisprudence and international standards (Table 5) highlights a gap in the protection of digital correspondence.

Table 5. Jurisprudential gap between Albanian court cases and international standards.

Proportionality Variable	Albania (160 decisions)	Italy	ECtHR (Art. 8)	Gap
Classified as correspondence	0%	100%	100%	-100 pp
Prior judicial authorization	4.4%	100%	100%	-95.6 pp
Scope limited ex ante	0%	100%	75%	-75 pp
Data destruction orders	0%	100%	25%	-25 pp
Average proportionality score	0.14	3.50	3.00	-2.86

The data collected by SPAK in 2024 show that mobile phones accounted for 65.8% of all digital evidence collected for forensic testing and there were still 209 confiscated devices waiting to be tested. This shows that the use of digital evidence is increasing and that there is an increasing need for unified approach from the courts on how such evidence should be assessed according to international standards [29].

Hypothesis Testing

Table 6 depict hypothesis used in the study.

Table 6. Hypothesis

H	Hypothesis	Evidence	Status
H1	Mobile phone data treated as correspondence only when judicial authorization required	0% classified as correspondence; 4.4% judicial authorization; Fisher $p<0.001$	Confirmed
H2	Weak proportionality due to lack of structured classification	Mean score 0.14 vs 2.00	Confirmed

Variable Operationalization and Proportionality Score Construction

In order to ensure methodological transparency and reproducibility, all variables that are used in the empirical analysis are defined operationally in Table 7.

Table 7. Operational variable definitions

Variable	Operational Definition	Coding (Score)	Legal Basis
V1 – Correspondence Recognition	Court decision explicitly classifies mobile device data as protected correspondence under Art. 36 of the Constitution, or Art. 8 of the ECHR.	Yes =1 No = 0	Art. 36 of the Albanian Constitution; Art. 8 of the ECHR; Constitutional Court Decision No. 44/2025.
V2 – Prior Judicial Authorization	A judicial order issued specifically authorizing access to digital data on the device prior to or at seizure, distinct from general search warrant	Yes = 1 No = 0	Art. 208/a of the Albanian CPC; Riley vs. California (2014); ECtHR Kruglov vs. Russia (2020)
V3 – Ex Ante Scope Limitation	Judicial order or prosecutorial decision explicitly limits the scope of data search to specific offense, time period, or data category prior to examination	Yes = 1 No = 0	Barak proportionality necessity test [12]; ECtHR Big Brother Watch vs. UK (2018).
V4 – Data Destruction Order	Court or prosecutor orders the destruction or return of irrelevant data extracted during examination.	Yes = 1 No = 0	Directive (EU) 2016/680; ECtHR Zakharov vs. Russia (2015); CJEU Case C-548/21 (2024).
Proportionality Score (PS)	PS = V1 + V2 + V3 + V4; Range 0–4. Higher scores indicate greater alignment with constitutional proportionality standards.	0 – 4 composite	Barak four-stage proportionality model [12]; Alexy balancing theory [54].

The proportionality score (PS) is a composite indicator obtained from four binary sub-variables, each coded 0, or 1: (i) recognition of the device as correspondence; (ii) existence of prior judicial authorization; (iii) ex ante scope limitation; and (iv) existence of a data destruction order.. The PS for each decision equals the sumtotal of these four binary values (sub-variables), yielding a scale of 0–4. A score of 0 indicates no proportionality safeguard was applied; a score of 4 indicates full compliance with a structured proportionality framework. This logical approach is consistent with Barak's four-stage proportionality model [12] and it enables a direct comparison with the foreign jurisdictions coded on the same variables.

The Inter-coder Reliability was assessed on a 20-case sub-sample by a second independent coder, yielding a Cohen's Kappa of $\kappa = 0.84$ (strong compliance) across the four binary variables. Weak compliance arose primarily in V3 (Scope Limitation), where implicit rather than explicit limitations were ambiguous; in such cases the conservative code (0) was applied. All the coding decisions as well as the codebook are available from the corresponding author upon request, ensuring full reproducibility.

Falsifiable Hypothesis Redesign

The two central hypotheses of this study are reformulated here in falsifiable terms, with explicit competing explanations and stated refutation conditions, in response to reviewer critique. This reformulation does not alter the substantive findings reported above; it clarifies the falsifiability structure underlying the analysis.

H1 (Revised – Falsifiable Form): In Albanian criminal proceedings, the legal classification of a mobile device as "computer data" (rather than "material evidence") is a necessary and sufficient condition for the issuance of a prior judicial authorization for data access. The hypothesis would be refuted if: (a) a substantial proportion of decisions (≥20%) classified devices as material evidence but still issued a judicial data access order; or (b) devices classified as computer data failed to generate judicial authorization in ≥20% of cases. Under competing explanation CE1 (institutional inertia hypothesis), the absence of judicial authorization reflects not the classification logic but instead the prosecutorial culture of minimizing procedural steps. Under competing explanation CE2 (legislative gap hypothesis), the absence reflects the inadequacy of Art. 208/a CPC rather than deliberate classification choices. The Fisher's Exact Test result ($p < 0.001$) and the 0% judicial authorization rate in the material-evidence category falsify CE1 and CE2 as the primary explanatory mechanism: classification drives authorization, not procedural culture alone.

H2 (Revised – Falsifiable Form): Albanian courts applying a material-evidence classification will produce a significantly lower proportionality score (PS) than courts applying a computer-data classification. The hypothesis would be refuted if the Mann–Whitney U test failed to detect a statistically significant difference ($p \geq 0.05$) in PS distributions between the two classification groups, or if effect size (Cohen's d) fell below a medium threshold ($d < 0.5$). Competing explanation CE3 (offense-severity hypothesis) holds that PS differences reflect the severity of the underlying offense rather than classification. This is addressed by the absence of any PS variation within the material-

evidence group (PS = 0.00 uniformly), which cannot be explained by offense severity alone. Competing explanation CE4 (post-2021 reform hypothesis) holds that the 2021 Supreme Court decision drives any observed improvement, independently of classification.

Temporal sub-analysis (pre-2021 vs. post-2021 decisions) shows modest but directionally consistent improvement, not a structural discontinuity, which limits the scope of CE4. The Mann–Whitney result ($p < 0.001$, $d > 2.0$) confirms H2 under these conditions.

Taken together, H1 and H2 are confirmed by the empirical data: Fisher's Exact Test ($p < 0.001$) establishes that legal classification is the operative driver of judicial authorization, and the Mann–Whitney result ($p < 0.001$, $d > 2.0$) confirms that this classification produces a large and statistically significant difference in proportionality outcomes. The competing explanations CE1 through CE4 are not falsified outright but are shown to operate as secondary factors rather than primary causal mechanisms. These results are interpreted in detail in the Discussion section below, where they are positioned against SOTA benchmarks.

Unlike prior SOTA studies, which assume proportionality as a baseline condition, the present hypotheses explicitly test whether that baseline exists at all in a post-transition legal system.

Methodological Limitations

The main limitation of this research is the limited access to court decisions within the Albanian legal system. The electronic registry used by district courts did not provide access to the decisions of the courts of first instances [42-48]. The study had to rely on archival materials from a limited number of prosecution offices.

Therefore, from the statistical aspect, the sample of 160 case files cannot be considered as a national representative and should be considered as a suggestive sample. However, the patterns observed across this relatively large group of cases suggest the presence of a trend overall rather than an isolated exclusion. It is suggested that to have a more accurate picture, a larger and more comprehensive sample of court cases should be included in the analysis combined with interviews with judges, prosecutors, and digital forensic practitioners of all level courts and regions [1, 8].

NOVELTY, RESEARCH GAPS, AND CONTRIBUTIONS RELATIVE TO SOTA

Novelty Claims

This study introduces several original contributions that extend beyond the current state of the art (SOTA) [49-55]. The central and most defensible novel contribution is the Proportionality Score (PS) instrument, a four-variable composite index (V1+V2+V3+V4, range 0–4) derived from Barak's four-stage proportionality model [12] and operationalized against a real dataset of 160 judicial decisions. Unlike Barak's original framework, which presupposes that Stage 1 (proper constitutional recognition) is already satisfied, the PS

instrument is explicitly designed to diagnose cases where Stage 1 is absent what this study terms the "pre-proportionality failure mode." No existing SOTA study applies a scored, multi-variable proportionality instrument to real case-level data in any post-transition legal system; the PS instrument thus fills a methodological gap that theoretical frameworks (Barak [12], Kerr [10], Nissenbaum [11]) leave open. A second original contribution is the four-model typology (Models A–D), which classifies jurisdictions by their dominant constitutional-procedural logic rather than by geography, enabling structural comparison across systems at different stages of digital rights development. Together, these two contributions PS instrument and A–D typology constitute original analytical tools, not merely applications of prior frameworks. The remaining contributions are described below:

- *First empirical dataset on Albania (160 cases, 2017–2025)*: Unlike predominantly doctrinal SOTA studies, this research provides quantitative evidence on judicial practice in a post-transition legal system.
- *Operationalization of proportionality*: The study translates abstract constitutional doctrine into a measurable proportionality scoring framework, enabling statistical testing.
- *Reclassification paradigm*: It advances a normative and doctrinal argument that mobile phone data constitute "correspondence", bridging constitutional law and digital forensics.
- *Empirical–theoretical integration*: Combines privacy theory (Nissenbaum, Solove), proportionality (Barak), and mosaic theory (Kerr) into a unified analytical model applied to real case law.
- *Identification of systemic procedural gaps*: Demonstrates a near-total absence of judicial authorization (95.6%), a finding not previously quantified in regional literature.
- *Comparative constitutional positioning*: Situates Albania within European and ECtHR standards, revealing measurable divergence using structured indicators.

Unlike existing SOTA approaches, which remain either doctrinal (e.g., ECtHR jurisprudence, Barak's proportionality theory) or descriptive (comparative legal analyses without measurable outputs), the Proportionality Score (PS) introduced in this study provides a replicable, case-level measurement tool that quantifies constitutional compliance. Existing literature does not allow ranking, comparison, or statistical testing of proportionality across decisions. By contrast, the PS enables direct comparison across jurisdictions and over time, transforming proportionality from a purely normative concept into a testable empirical variable. This shift from descriptive to measurable analysis constitutes the study's primary methodological innovation.

Research Gaps in the Literature

Despite extensive scholarship on digital privacy and evidence [56-62], the following gaps are not merely declared but are directly demonstrable from the SOTA literature itself:

- Lack of empirical validation: Most SOTA studies do not test how legal principles operate in practice at the level of individual decisions. Authors in [7] provide no

coded dataset; Stoilkovski [8] offers normative guidelines without case-level evidence; Bernardini [1] surveys jurisprudence without frequency data. The consequence is that the assumption of proportionality compliance cannot be verified or falsified without empirical case coding. The present dataset (n=160, coded on V1–V4) is the first to make this assumption testable in a post-transition context, finding it is systematically false (V1=0%, V2=4.4%).

- Geographical limitation: The SOTA literature explicitly acknowledges this boundary. Authors in [7] limit applicability to "mature democracies." Bernardini [1] covers EU member states only. Stoilkovski [8] covers OSCE guidelines but provides no country-specific case data for Balkan jurisdictions. The gap is not merely geographical but structural: post-transition legal systems may follow a different convergence trajectory, a hypothesis that existing SOTA cannot test because it lacks the data. The present study provides the first empirical test of this hypothesis for Albania, with results that challenge the convergence assumption.
- Absence of measurable frameworks: Barak's four-stage model [12] is the dominant proportionality framework in SOTA, but no existing study translates its four stages into binary variables applied to a real dataset. Kerr [10] develops mosaic theory conceptually; Nissenbaum [11] develops contextual integrity philosophically. Neither produces a scoring instrument generating numeric output comparable across cases and jurisdictions. The PS instrument introduced here fills this gap: it converts Barak's four stages into V1–V4, enabling mean PS of 0.14 (Albania) to be directly compared with 1.40 (Italy pre-2023), 3.30 (Italy post-2023), and 3.75 (ECtHR/CJEU).
- Fragmentation between law and technology: Technical forensics literature (Horsman [14], Punja and Mislan [31]) documents extraction procedures without engaging constitutional proportionality. Constitutional scholarship (Barak [12], ECtHR doctrine) develops rights frameworks without engaging technical realities such as encryption thresholds, metadata aggregation, and cloud synchronization. The present study bridges this divide by integrating forensic architecture analysis directly into the proportionality argument, demonstrating that technical decisions at the seizure stage carry direct constitutional implications that existing literature treats as separate domains.
- Limited focus on classification problem: The legal distinction between material evidence and digital correspondence is the operative driver of proportionality outcomes in this study (Fisher's $p < 0.001$), yet no existing SOTA study identifies this classification choice as a primary research variable. Newell and Koops [7] assume correspondence classification; ECtHR doctrine assumes it; Barak [12] assumes it. None asks what happens when classification itself is the problem — which is precisely the Albanian configuration. The present study demonstrates that the classification decision is not a preliminary step but the central determinant of

all downstream proportionality analysis, a finding with direct implications for any transitional system facing similar classification inertia.

This study directly addresses each of these gaps through a data-driven, comparative, and operationalized approach [63-67]. Critically, the gaps are not additive but structurally connected: the absence of empirical validation (Gap 1) in the geographical blind spot (Gap 2) means that the conceptual frameworks (Gap 3) have never been tested in the context where they matter most for EU convergence — post-transition legal systems where the baseline constitutional recognition these frameworks assume may not exist. The PS instrument addresses all five gaps simultaneously: it is empirical (Gap 1), applied to a post-transition jurisdiction (Gap 2), operationalizes proportionality into measurable variables (Gap 3), integrates forensic and constitutional analysis (Gap 4), and places the classification problem at the center of the research design (Gap 5).

This gap is not merely asserted but demonstrable from the SOTA literature itself. For instance, Newell and Koops explicitly limit their conclusions to "mature democracies," thereby excluding post-transition systems such as Albania. Similarly, Stoilkovski provides normative guidelines without any coded dataset, making empirical validation impossible, while Bernardini surveys European jurisprudence without producing frequency-based or case-level data. As a result, none of these studies can verify whether proportionality is actually applied in practice. The present dataset (n=160) directly addresses this limitation by transforming these assumptions into empirically testable claims.

Comparative Positioning Against SOTA

The studies most directly comparable to this research are [1, 7, 8, 68-70]. Each represents genuine SOTA work, but each is methodologically bounded in ways that the present study directly overcomes. Newell and Koops conduct the most rigorous transatlantic comparison available, but their analysis is entirely doctrinal: it generates no case-level data, produces no quantitative measure of compliance, and explicitly excludes post-communist jurisdictions. Stoilkovski provides practice-oriented OSCE guidelines but contains no constitutional analysis and no coded decision data; it describes what should happen, not what does. Bernardini surveys European jurisprudential developments systematically but covers only EU member states and offers no frequency data. The common limitation across all three is the same: they cannot distinguish between a jurisdiction that formally recognizes a constitutional principle and one that applies it in practice. The PS instrument introduced in this study makes exactly this distinction operational. A jurisdiction that recognizes correspondence protection (V1=1) but never requires prior judicial authorization (V2=0) scores PS=1 or less, a configuration no prior study could detect or measure.

Table 8 below summarizes the comparative positioning; the analytical superiority of the present study lies not in broader scope but in methodological precision: it converts the normative claims of the SOTA literature into empirically falsifiable propositions and tests them against real judicial decisions.

To enhance external validity, a targeted comparative dataset (n ≈ 20–30 cases) from Italian jurisprudence and ECtHR case law was coded using three core variables:

- Recognition of correspondence (Yes/No)
- Judicial authorization required (Yes/No)
- Scope limitation (Ex ante restrictions present/absent)

Table 8. Comparative data in relation to SOTA

Study	What They Do	Limitations	What This Study Adds
[68]	US–EU comparison of smartphone searches	No empirical dataset; excludes SE Europe	Adds empirical evidence from Albania+ proportionality metrics
[69]	Cybercrime investigation standards	Limited constitutional analysis	Links forensic practice with constitutional safeguards
[70]	European comparative procedural law	No focus on transitional systems	Introduces post-transition empirical jurisprudence
[71]	ECtHR doctrine on correspondence	No application to mobile devices	Applies doctrine to mobile data classification problem
[10]	Mosaic theory	US-centric, theoretical	Empirically validates aggregation risks in practice
[11, 72]	Privacy theory frameworks	No procedural/legal application	Integrates theory into criminal procedure and case law

Table 9 depict the comparative data between Albania, Italy and ECtHR

Table 9. Comparative data: Albania vs Italy vs ECtHR

Variable	Albania (n=160)	Italy (n≈25)	ECtHR Standards
Recognition as correspondence	0%	~100%	100%
Judicial authorization	4.4%	100%	100%
Scope limitation	0%	~90–100%	~75%

The comparative results confirm a systemic divergence between Albanian practice and European constitutional standards. While Italian courts and ECtHR jurisprudence consistently require prior judicial authorization and ex ante scope limitation, Albanian courts overwhelmingly classify devices as material evidence, bypassing safeguards. This divergence is not merely doctrinal but structural, reflecting a misalignment between legal classification and technological reality, which directly affects proportionality outcomes.

To clearly position this research within the current State-of-the-Art (SOTA), Table 10 summarizes how this study addresses specific gaps that are not covered by existing literature, particularly regarding the Western Balkan legal landscape. The key analytical distinction is the following: while each SOTA comparator contributes valuable doctrinal, normative, or theoretical analysis, none produces a quantitative output that allows compliance levels to be ranked, compared, or tracked over time. The present study produces such an output (PS = 0.14 for Albania vs. 3.30 for Italy post-2023 vs. 3.75 for

ECtHR/CJEU). This numeric comparability is the methodological contribution that makes this study analytically superior within its domain — not because it covers more ground, but because it converts normative claims into falsifiable, replicable measurements

Table 10. Summarizes how this study addresses specific gaps

Study	Focus Area	Methodology	Main Contribution	Gap Addressed by This Paper
[68]	US/EU Perspective	Comparative Legal Analysis	Privacy in smartphone searches.	Lacks empirical data from transitional Balkan jurisdictions.
[69]	OSCE Guidelines	Policy Review	Procedures for cybercrime investigation.	Focuses on guidelines, not on judicial application (court rulings).
[70]	EU Digital Evidence	Jurisprudential Review	Seizure of electronic devices in EU.	Does not cover non-EU candidate countries like Albania.
[63]	Human Rights	Theoretical Analysis	Encryption and privacy rights.	Primarily theoretical; lacks quantitative empirical backing.
[5]	Case Law C-548/21	Judicial Precedent	Access to data vs. crime gravity.	Focuses on EU law; needs local context for implementation.
This Study (2026)	Albania	Empirical (160 cases)	Proportionality Index (PI)	First empirical dataset for Albania; bridges local law with ECtHR SOTA.

Additionally, the original Table 9 presented Italian data as uniformly "~100%" across all variables. Following direct online verification of 23 Italian decisions (Corte Costituzionale and Corte di Cassazione, sourced from cortecostituzionale.it, giurcost.org, eius.it, sistemapenale.it, studiovigna.it, lexced.com) and 8 ECtHR/CJEU rulings (HUDOC, bailii.org, curia.europa.eu), Table 9 is revised below in Table 11 to reflect the actual coding per the operationalized variables (V1–V4) defined in Table 7.

Table 11. Verified Comparative Dataset (n=31): Albania vs Italy vs ECtHR/CJEU

Variable	Albania (n=160)	Italy pre-2023 (n=13)	Italy post-2023 (n=10)	ECtHR/CJEU (n=8)
V1 – Recognition as correspondence	0%	~15% (data treated as "document" under Art. 234 c.p.p.)	100% (after Sent. 170/2023)	100%
V2 – Prior judicial/administrative authorization	4.4% (7/160 cases)	~100% (PM decree, Art. 253–254 c.p.p. — no case found without authorization)	~100% (debate: PM vs GIP after CJEU C-548/21)	100% (independent judicial body required)
V3 – Scope limitation ex ante	0%	~85% (mandatory from Cass. n. 53168/2016)	100%	~75–100%

Mean PS	0.14	1.40	3.30	3.75

The critical methodological distinction identified through this verification is the following: Italy has always required some form of authorization (V2≈100% throughout, through the Pubblico Ministero decree under Art. 253–254 c.p.p.); however, classification of data as constitutionally protected "correspondence" (V1) only became universal after Corte Costituzionale Sent. n. 170/2023. Albania, by contrast, shows V2=4.4% and V1=0% for the entire period 2017–2025. The structural gap is thus located primarily in V2 and V3, not only in V1.

The revised data reveal a more nuanced but analytically stronger picture than the original Table 7. The structural gap between Albania and Italy is located primarily in V2 (authorization: 4.4% vs ~100%) and V3 (scope limitation: 0% vs ~85–100%), not only in V1. Even before the landmark Corte Costituzionale Sent. n. 170/2023, Italian prosecutors were always required to issue a motivated seizure decree specifying the investigative scope (Art. 253–254 c.p.p.), and indiscriminate "a strascico" seizures had been judicially prohibited since Cass. n. 53168/2016. Albania lacks both requirements entirely. The V1 gap (correspondence classification: 0% AL vs ~15% IT pre-2023 vs 100% IT post-2023) confirms the "pre-proportionality failure mode" identified in Section 5.3 above. This revised analysis does not weaken the paper's central thesis — it strengthens it by demonstrating that the Albanian deficit is multi-dimensional and structural.

Expanded Limitations

This study is subject to several limitations which are as follows:

First, the sample size (n=160), while substantial, is not fully representative of all Albanian jurisdictions due to restricted access to first-instance court decisions. This may introduce selection bias.

Second, the comparative dataset (Italy and ECtHR) is limited in size and relies on purposive sampling, which constrains generalizability but still provides indicative benchmarking.

Third, the proportionality scoring system, although systematic, involves a degree of interpretative judgment in coding legal reasoning, which may affect reproducibility.

Fourth, the study does not evaluate the quality or reasoning depth of judicial decisions, focusing instead on measurable procedural safeguards.

Additionally, rapid technological evolution in mobile data ecosystems may outpace current legal frameworks, meaning that findings should be interpreted as time-bound within the 2017–2025 period.

Future research should expand datasets across jurisdictions, incorporate automated legal text analysis, and explore causal mechanisms between legal classification and rights protection.

Despite the rigorous methodology applied, several limitations must be acknowledged to provide a transparent context for the findings of this research. These limitations

primarily stem from the challenges of accessing judicial data, the specific characteristics of the sample, and the evolving nature of digital forensics.

A primary constraint encountered during this research was the lack of a fully centralized and digitized judicial archive in Albania. Accessing court decisions, particularly those involving search and seizure orders, proved challenging due to the fragmented nature of judicial record-keeping. Many decisions are still stored in physical archives or in internal systems that are not easily searchable via keywords related to "digital evidence" or "computer data." Consequently, the process of data collection relied on manual identification and physical access to court registries, which may have limited the inclusion of older cases or those from smaller, more remote district courts.

The study is based on an empirical analysis of 160 judicial decisions. While this dataset is the largest of its kind for the Albanian jurisdiction and provides a statistically significant baseline, it may not capture the full diversity of judicial reasoning across all levels of the judiciary. Most decisions analyzed were from major urban centers, where cybercrime and digital forensics are more frequently litigated. Therefore, the findings might reflect a more "urbanized" judicial perspective on digital privacy, potentially overlooking different trends in smaller courts where digital evidence might be handled with less technical scrutiny.

Another limitation lies in the brevity of the court orders themselves. In many instances, judicial authorizations for search and seizure are standardized and provide limited detail regarding the technical debate that may have occurred in the courtroom. This "standardized language" often obscures the depth of the proportionality assessment carried out by the judge. As a result, the analysis is limited to the written justification provided in the final order, which may not always reflect the full complexity of the arguments regarding the necessity and intrusiveness of the data seizure.

The rapid pace of technological advancement presents a constant challenge for legal research. The digital forensics tools used by law enforcement during the period covered by the 160 cases are constantly evolving. Limitations in the study include the inability to verify the exact technical methods used for data extraction (e.g., full-disk imaging versus logical extraction) for every case, as these details are often missing from the judicial record. Furthermore, this study reflects the jurisprudence up to early 2026; subsequent shifts in practice following the full implementation of recent Constitutional Court decisions may alter the landscape in ways not fully captured by this dataset.

Finally, while the study incorporates a comparative analysis with Italian and ECtHR jurisprudence, the legal interpretation remains focused on the Albanian Constitutional framework. The findings are intended to be a case study for transitional democracies, but the specific legal outcomes are inherently tied to the nuances of the Albanian Criminal Procedure Code, which may limit the direct transplantability of the results to other jurisdictions without accounting for local procedural variations.

MOBILE DEVICE FORENSICS: A DYNAMIC PARADIGM

Mobile device forensics deals with the extraction of digital evidence from modern mobile devices such as smartphones and tablets [31, 37, 38]. It involves not only retrieving data but also storing, preserving, and documenting the evidence in a way that allows it to be used in court [31, 36].

Unlike traditional computer systems, mobile devices are rarely isolated. They constantly interact with networks, satellites, and other devices. As a result, the data they contain is often dynamic. A mobile phone may continuously communicate with mobile towers, Wi-Fi networks, GPS satellites, Near-Field Communication (NFC), and other systems. The many applications and communication channels found on these devices make them a rich source of personal information. At the same time, this raises concerns about the protection of evidence and the safeguarding of constitutional rights [11-13, 36].

For this reason, mobile device forensics differs in important ways from traditional computer forensics. Evidence from mobile devices can be distributed across different systems and closely connected to many aspects of a person's private life. This makes it necessary to have procedures that keep pace with technological developments, operate within legal limits, and respect the right to privacy [35, 36].

To make it clearer, the forensic process follows four key stages of proceedings (seizure, capture, analysis and reporting); however, each step involves constitutional questions beyond their technical implementation. The seizure is the first stage where rights are likely to be violated. There is no pre-determined procedure for the judicial police or prosecutors in Albania in terms of how to secure the device while ensuring data integrity and admissibility [5, 64]. Devoid of any formal procedures, practices may not respect the constitutional values of correspondence protection, right to privacy and proportionality [9, 10, 12].

The last stages, data acquisition/image, refers to cloning the sector of a number of the devices. Hashing algorithms are used to authenticate and forensic analysts decide the direction of the investigation. In the analysis phase, the available and unallocated memory is carefully managed using software to find the relevant information. Lastly, the reporting stage, requires producing a report on all findings in a reproducible manner based on the concept of audit trail [31, 36]. The stages in forensic practice include technical and normative aspects.

The qualitative distinctions between conventional searches and those of the smartphone are, in terms of their analytic impact, the defining factors of this difference. Chief Justice John Roberts (Supreme Court, USA) emphasized that likening the search of a smartphone or the access to its digital contents to a search of a physical object fundamentally misconstrues the nature of 'the information age' noting that 'comparing a search of digital contents to a search of a physical object is akin to likening a horseback ride to a flight to the moon' [7, 26]. Searching pockets or a bag may be a minor inconvenience whereas rummaging through the contents of a smartphone involves much more [35].

The aggregation principle reinforces constitutional theory by demonstrating how aggregated bits, visible to the human eye as less than innocent, represent comprehensive portraits of one's private life and thus require more stringent procedural safeguards. Countries across the globe have acknowledged this distinction courts in Canada and the UK, for example, have frankly conceded 'no analogy can be drawn between a search of a mobile telephone and a search of items in the home or other premises' [7, 26, 41-43].

In Albania prosecutors can face significant legal and practical problems when seizing mobile phones in the context of investigating serious offenses such as corruption, organized crime and money laundering. Two main procedures are used, namely seizure as material evidence, where an Expert conducts an examination appointed by the judicial police without prior Judicial approval and seizure as computer data (Article 208/a, Criminal Procedure Code), a more selective procedure [19, 31, 50].

The common practice of approaching mobile devices as material evidence evidences a disconnection between technological realities and constitutional protections. This approach often takes certain aspects of the recognition of the right to correspondence proportionality review and formal recognition and circumvents their application in practice, posing normative questions on whether investigations respect Human Rights norms [9, 10, 12, 18].

The evidence presented in the previous sections shows that this is often not the case. Even though we have technological tools and the information is very personal, mobile phones are seldom seen as protected correspondence. The few cases where prior approval is sought suggest that the procedures used are not consistent and lack a clear approach to searches and privacy. Overall, the forensic, empirical, and legal views in this research indicate that mobile devices bring both opportunities and challenges. They serve as sources of information and store significant amounts of personal data. It is still unclear if the Albanian legal system can meet the rising demand for procedures that are legally sound and technically reliable.

The analysis indicates that this needs clearer legal guidelines, careful assessments of proportionality, and a more active role from the courts. When forensic practices are conducted within a framework that respects fundamental rights, investigators can better balance the needs of criminal investigations with the protection of privacy, communication, and due process. In this way, evidence, technology, legal procedures, and fundamental rights must develop together and remain closely linked.

DISCUSSION

Quantitative Findings in Light of Albanian Jurisprudence

Further quantitative analysis of a sample of 160 Albanian court decisions concerning mobile phone data uncovers a pattern of consistent and problematic handling of the evidence by courts. As well as 153 decisions (95.6 %), courts treated cellular phones as physical material evidence of the contents under failed prior judicial authorization, and

only 7 decisions (4.4 %) ordered computer evidence to be seized [19, 28]. Curiously, the decisions did not recognize the mobile device as protected correspondence under Article 36 of the Albanian Constitution at all (0 %). This yielded an overall mean proportionality score of 0.14, failing to indicate any concern with proportionality or alternative procedural safeguards [18, 53, 54].

The more recent empirical evidence confirms that as a matter of practice, the investigation of digital evidence in Albania has not emphasized procedural safeguards but resorted to expedience. As a practical matter, this "shallowness of approach" has disregarded the qualitative and quantitative distinctiveness of the information stored in mobile devices which is in two ways highly personal and of course summated [35, 36]. This evidence therefore serves as a useful benchmark against which to compare recent jurisprudential progress and the conformance of Albanian practice to the constitution and relevant international standards.

The Supreme Court's Unifying Decision No. 147 (22 December 2021) indicates a positive focus on codifying proportionality in data seizures [28]. Therefore, the Supreme Court sets out concrete measuring criteria for core elements of proportionality, including whether seizure is intended to be the reason to examine necessity, suitability, and balancing; the Court also notes that all seizure must be "reasoned, reasonably limited, and within the scope of the investigation," and that mobile devices should not be conceptualized as computer systems. Although the Court, classifies mobile phones as a material object, the Supreme Court's reasoning focus on specificity and proportionality in extraction suggests that courts ought to avoid unstructured classification and undertake a careful, dignity preserving analysis of digital evidence that can improve upon the dataset's low scores (0.14) [28, 36].

A more substantive step can be identified in respect of the Constitutional Court Decision No. 44 of 29 July 2025 where the Court explicitly included mobile phone data within the scope of the protection under Arts 35 and 36 of the Constitution and Art 8 of the European Convention on Human Rights [18, 20, 29]. The Court found that the copying or copying out or the inspection of all data stored on a phone without "an investigative link" constituted a violation of the secrecy of correspondence. This decision established a qualitative difference between searches of physical property and searches of digital property by reiterating that a search of digital data must have "specific and sufficient reasons", a standard akin to the proportionality requirement which can be considered extensive and yet even beyond international case law. The Court expanded from this precedent and validated layered judicial authorizations for both the physical search and the subsequent digital search of data [26, 29, 36]. However, this two-layered approach of the court has made this tool of investigation very complex and very difficult to yield the expected result as the digital evidence can be erased by the suspect online.

While these judicial developments can be considered a positive trend in Albanian case law, the concern as mentioned above, especially in the case of the Constitutional Court Decision raises concerns on their applicability in terms of the fight against organized crime

and high-profile corruption. The Supreme Court supplies procedural scaffolding for the principle of preserving proportionality and specificity (the Court's decisions provide the framework for most of the reasoning) and the Constitutional Court provides a very extensive assurance that digital data protection is guaranteed in the Constitution and human rights [28,29,36]. Their true effect will be seen in practice but could include the slight narrowing of the empirical gaps found namely the near total absence of savings classification and judicial oversight [45, 46]. The 4.4% of cases a judicial affirmation received, had an average proportionality score of 2.00.

These judicial developments are analytically significant, but their theoretical implications must be assessed against SOTA benchmarks rather than evaluated in isolation. Kerr's mosaic theory [10] predicts that as courts begin to recognize the aggregation problem, proportionality reasoning will emerge organically from doctrinal evolution. The Albanian data provide a partial test of this prediction: the Supreme Court's Unifying Decision No. 147/2021 introduced aggregation-sensitive language, yet the post-2021 sub-sample does not show a structural discontinuity in PS scores — the 4.4% judicial authorization rate and PS = 0.14 remain essentially stable. This constitutes a meaningful disconfirmation of Kerr's convergence assumption: doctrinal awareness of aggregation does not automatically translate into measurable proportionality outcomes in a post-transition legal system. The implication, consistent with Newell and Koops [7], is that explicit legislative operationalization — not judicial evolution alone — is necessary to produce structural change [53, 55].

The Constitutional Court Decision No. 44/2025 represents a qualitatively different intervention: unlike the Supreme Court's procedural guidance, it establishes a constitutional baseline (V1 = recognition as correspondence) that was absent in 100% of the pre-2025 dataset. If consistently applied, this decision would shift the Albanian system from Barak's Stage 0 — the pre-proportionality failure mode identified in this study — to at minimum Stage 1, enabling downstream proportionality analysis at Stages 3 and 4. Whether this constitutional mandate translates into measurable PS improvements in post-2025 decisions remains an empirical question that future research should address through replication of this study's coding methodology on a prospective dataset. For the period under review (2017–2025), the quantitative data support only a cautious conclusion: jurisprudential progress is real but structurally insufficient to close the measured gap, see Table 12 [18, 19, 45, 46].

The findings indicate a systematic divergence between the requirements of Article 36 of the Constitution and current judicial practices. Rather than a mere procedural oversight, this suggests a doctrinal lag in recognizing digital data as a distinct form of correspondence. The data suggests that courts prioritize investigative efficiency, often at the expense of the strict proportionality standards established by the ECtHR in cases like Saber v. Norway.

These findings challenge a core assumption in the SOTA literature, particularly the convergence hypothesis suggested by comparative studies (e.g., Newell & Koops),

according to which legal systems gradually align with ECtHR standards through doctrinal evolution. The Albanian data provide a counter-example: despite clear constitutional and international standards, no structural convergence is observed (PS = 0.14; 0% recognition of correspondence). This suggests that doctrinal awareness alone is insufficient to produce compliance, and that institutional or classification-based constraints may play a more decisive role than previously assumed

Table 12. Legal Classification of Cellular Devices, Judicial Oversight, and Alignment with Recent Albanian Jurisprudence

Legal Classification	% of Cases (N=160)	Judicial Authorization	Average Proportionality Score	Alignment with Recent Jurisprudence
Physical/Material Evidence	95.6%	None (0/153)	0.00	Supreme Court UD 147/2021 encourages careful seizure; CC 44/2025 promotes rights protection
Computer Data Seizure	4.4%	Yes (7/7)	2.00	Fully aligned with proportionality and judicial oversight principles
Recognized as Correspondence	0%	N/A	N/A	CC 44/2025 establishes constitutional basis for recognition and protection

TECHNOLOGICAL DIMENSION AND MOBILE DATA ARCHITECTURE

A comprehensive analysis of the proportionality of mobile device data requires engagement with the technological realities that underpin the legal argument. The constitutional importance of fundamental human rights related to smartphone data cannot be assessed in isolation from the technical architecture that determines what data are generated, stored, and accessible to forensic investigators. This section provides the technological analysis necessary to support the legal conclusions in this paper.

Mobile Data Architecture and Storage Layers

Enabling smart devices to use cellular internet has created a suitable ground for a large number of mobile applications. In the past, cell phones were used mainly for communication, but currently they (smartphones) can be used to perform many different tasks, such as games, internet browsing, multimedia functionalities, and use of applications [58]. This makes cell phones to generate large amounts of data, which can be used to gain useful insights about the user [59]. All these devices generate massive amounts of structured and unstructured data called Mobile Big Data. These data move rapidly and

vary in value, meaning, and formats. They also come from many different sources (e.g., social media networks, sensors, applications).

Mobile Big Data are not an entirely new concept, as they stem from Big Data and share some similarities with them, but there is still no specific architecture for Mobile Big Data. In general, Big Data include structured, unstructured, and semi-structured data [60], which must be processed by advanced analysis to uncover patterns, correlations, and other insights that can lead to better decisions [61]. Big Data often come from various sources and in multiple formats, which can make their analysis even more complex.

Modern smartphones operate across multiple distinct layers of data storage, each of which carries distinct significance within the framework of human constitutional rights. At the hardware level, internal NAND flash memory (typically 64–512 GB in contemporary devices) stores the operating system, application data, and user-generated content within a physically integrated circuit that is inseparable from the device itself. UICC/SIM cards, in contrast, store subscriber identity, contacts, and limited message logs within a removable module governed by separate telecommunications regulation. External microSD cards, when present, can contain data such as photos and videos, and various applications.

This layered architecture has direct implications on fundamental human rights and freedoms. The principle of aggregation, which is articulated above, is not simply a theoretical proposition; it reflects the current technical reality, in which smartphones simultaneously store communications (WhatsApp, SMS, email), location history (GPS logs from mapping applications), biometric data (fingerprint and facial recognition templates), financial transaction data (mobile payment applications), health monitoring data (step counters, heart rate monitors), and comprehensive browsing histories. The technical capacity of a modern device to store, cross-reference, and reconstruct these data transforms a single forensic acquisition into a comprehensive biographical profile of the user.

Encryption Standards and Their Legal Significance

Contemporary smartphones implement full device encryption by default, using AES-256 encryption standards integrated at the hardware level via dedicated security chips (Apple Secure Enclave; Android StrongBox). This technical aspect creates a significant constitutional threshold [62]. Without user passcode or biometric authentication, forensic access to device content is virtually impossible, even after seizure under legal procedures. This technical obstacle reinforces the constitutional requirement for prior judicial authorization. The investigating authority must articulate specific evidentiary bases not only to justify the seizure of the physical device, but also to justify the subsequent request for access credentials. The self-incrimination implications of compelled passcode disclosure directly interact with the proportionality framework applied in this study, creating a dual constitutional constraint on investigatory access to encrypted cellular data.

The free use of encryption technologies is suggested by articles 11, 12, 19 and 27 of the Universal Declaration of Human Rights, i.e. the rights to be considered innocent, to privacy, to freedom of expression and to participate in scientific progress. A general ban

on an encryption method would need very strong arguments to counter this, for example, a structural increase in the risk of murder or physical harm in the absence of a ban. Since encryption in itself cannot cause bodily harm, in the event of a ban, punishment for its use is not expected to discourage anyone planning to inflict bodily harm on another person or group from taking such action. The effect of a ban would consist of the possibility of using encryption as an indicator for other illegal behaviour and to stop criminal intentions at the stage of using encryption in electronic communication.

However, the latter can also be achieved with more specific measures than a general ban on encryption, and can only work in an international framework, including internet governance stakeholders. Linking such a broad violation of fundamental rights to the benefit of crime reduction seems very inappropriate. Moreover, the current situation teaches us that the lack of (widespread) encryption encourages more criminal activity and enables groups and states to more easily violate fundamental human rights. In this aspect, encryption standards are not only important for preserving fundamental rights, but the free use of encryption constitutes a derivative universal right, while according to Article 12 of the UDHR (Universal Declaration of Human Rights) (and also Article 19 and Article 27) the UN member states are obliged to ensure the availability of encryption techniques whenever personal data is sent or received electronically within their territory [63].

Metadata Generation and the Aggregation Problem

Beyond the content of communications, modern smartphones automatically generate extensive metadata that often reveal more intimate information than the communications themselves. EXIF metadata, embedded in photographs, record GPS coordinates, timestamps, and device identifiers. Application logs store detailed data of user activity patterns. Network connection logs document physical movement through cell towers (offering location tracking without dedicated GPS). These metadata are generated passively, without intentional user action, and are constantly accumulated throughout the operation of the device. The constitutional importance is clear; a forensic examination that extracts only metadata, without accessing any communication content, can nevertheless reconstruct patterns of daily movement, social interactions, religious practice (participation in places of worship identifiable through location data), medical consultations, and political activities. This technical reality directly supports the proportionality argument throughout this paper, which should take into account the availability of targeted metadata extraction as an alternative to full device imaging.

Cloud synchronization and Flows of cross-border data

A technically and legally complex dimension of modern smartphone forensics is the automatic synchronization of device data with cloud storage infrastructure located in foreign jurisdictions. iCloud (Apple), Google One, and OneDrive (Microsoft) constantly store device content on servers physically located in Ireland, the Netherlands, or the United States, each subject to different data protection regimes. The CJEU's decision in Case C-548/21 [5] directly addresses this cross-border dimension, determining that access to data

stored on servers in another Member State requires judicial authorization in the requesting state in accordance with the requirements of the EU Charter.

This creates a technical-legal asymmetry with implications for the principle of direct proportionality. The Albanian investigative authorities conducting a complete forensic extraction of a seized mobile device may access data stored on foreign servers that have been downloaded to local memory, without realizing that different procedural requirements may apply. The legislative reform should clearly address this cloud synchronization dimension, requiring investigators to document whether the extracted data originate from local storage or cloud synchronization, and applying differentiated procedural requirements accordingly.

Comparative typology of jurisdictional models

The comparative jurisprudential analysis enables the construction of an analytical typology of jurisdictional approaches to the seizure of cellular devices. Instead of describing national systems sequentially, the typology places jurisdictions within four structural models based on their dominant constitutional and procedural logic. This analytical framework is original to this study and represents one of its main contributions to comparative constitutional studies.

***Model A**, as the Container-Based Model (the device as a physical object).* In this model, the smartphone is treated primarily as a physical object, material evidence that is subject to the general rules of seizure, provided for in Articles 187 et seq. of the Code of Criminal Procedure of Albania, without distinction between the device as a physical container and the data it contains. The medico-legal, forensic access to the content does not require judicial authorization beyond the initial decision of the prosecutor to seize the device. This model corresponds to the Albanian practice before 2024 (documented in 95.6% of empirical data), and the United States approach before the Riley precedent [39]. It offers maximum investigative flexibility, but provides minimal constitutional protection for data subjects, generating an average proportionality score of 0.00 (Table 8). The constitutional weakness of this model is its failure to account for the qualitative difference between seizing a physical container and accessing the intimate informational content of a digital life.

***Model B**, as the constitutionalized model of content,* recognizes the constitutional status of digital data protection independently of the physical device, treating the content of the smartphone as part of the protection of correspondence (or equivalent constitutional guarantee) and requiring specific judicial authorization for access to data, separate from the device seizure order. The United States jurisprudence after Riley and the Italian Constitutional Court [65] illustrate this model, which achieves an average proportionality score of 3.50 (Italy, Table 5.3). The strength of this model lies in the clear constitutional basis for data protection, but its operational challenge is determining the scope of authorized access within a specific investigation.

***Model C**, like the tiered authorization model,* is the most procedurally sophisticated model, requiring distinct judicial authorizations for different categories of data access: initial seizure; complete imaging/extraction; review of specific categories of data

(communications; financial data; location history). Austria's system following VfGH G-352/2021 [66] comes closer to this model, requiring prosecutors to specify the categories of data requested, and to demonstrate proportionality for each category independently. The CJEU's multi-stage proportionality analysis in Saber v. Norway (2021) [67] mirrors a similar tiered approach at the supra-national level. This model generates the highest intensity of proportionality review, but places the greatest procedural demands on the investigative authorities.

***Model D**, as a model of destruction and strong minimization of data:* This model fulfils the constitutional protection of content with mandatory requirements for the destruction of data after the investigation. Irrelevant data extracted during authorized forensic examination must be deleted within the stipulated timeframes, and the person must be notified of the examination and its scope. The Decree AS No. 806 (2024), proposed by Italy, moves towards this model, requiring the destruction of data "not relevant to the investigation" within 30 days of the completion of the forensic examination. This model addresses the temporal dimension of proportionality, the ongoing state intervention created by storing intimate data beyond its investigative usefulness, and is more in line with the data minimization requirements of the EU General Data Protection Regulation framework that Albania aspires to adopt.

The placement of jurisdictions within this typology, based on empirical data, reveals a clear pattern. Albania currently operates within Model A, a position that places it in systematic tension with ECtHR standards (Model C) and out of alignment with the trajectory of comparable jurisdictions. The reform recommendations below are specifically designed to facilitate Albania's transition from Model A to a hybrid Model B/C approach in line with its EU membership aspirations and constitutional obligations under Article 36 of the Constitution of the Republic of Albania.

THE ANALYSIS OF SENSITIVITY AND STABILITY

In order to assess the sustainability of the central argument, this section considers what would change if smartphone data were treated as digital documents instead of correspondence; and it considers key counter-arguments to the proportionality framework which are presented in this paper.

Alternative Classification: Digital Documents Instead of Correspondence

The main alternative to the classification of correspondence elaborated throughout this document is treating smartphone data as "digital documents," a category that would attract constitutional protection under various provisions (typically the right to privacy in the home or general privacy rights) but with potentially weaker procedural requirements. If this alternative classification were adopted, the implications would be: (1) lower threshold of protection, document searches in most jurisdictions require judicial authorization, but not necessarily the added protection given to correspondence; (2) broader permissible scope, document searches are usually authorized for defined categories without the

additional "targeting" requirement implied by correspondence protection; (3) reduced filtering requirements, return and segregation procedures mandatory for correspondence searches may not apply; and (4) weaker data destruction obligations, seized documents are usually held until trial without mandatory destruction of non-relevant material. This sensitivity analysis confirms that the classification of correspondence chosen in this paper, and supported by the case law of the ECtHR and the Italian Constitutional Court, and most recently by the Constitutional Court of the Republic of Albania, offers superior constitutional protection for data subjects. The doctrinal choice of the classification framework, therefore, is not neutral. It has direct practical implications for the level of procedural protection offered to individuals undergoing digital forensic investigation.

Counter-Arguments and Limitations

Three main counter-arguments to the principle of proportionality must be addressed.

Firstly, the weakening of investigative effectiveness. Tiered authorization requirements and mandatory data destruction impose a significant operational burden on prosecutorial authorities, potentially hindering the investigation of serious crimes, including corruption and organized crime, precisely the most prevalent categories in SPAK's practice in Albania (Special Prosecution Office against Corruption and Organized Crime).

This viewpoint has a practical basis, but it does not damage the proportionality framework. The balancing sub-test of proportionality expressly allows for the restriction of individual rights where the social benefit (effective crime investigation) is sufficiently important. The framework does not prohibit access to smartphone data. It requires structured justification and judicial oversight for that access.

Secondly, the objection to technological neutrality. The argument that constitutional protection should extend to all communication technologies regardless of the fact that it can be criticized as judicial law-making, replacing the intent of the drafters of the constitutions with contemporary functional analysis. This counter-argument underestimates the universal acceptance in constitutional studies and comparative jurisprudence that constitutions should be interpreted as living instruments, capable of addressing unforeseen technological developments [9].

Thirdly, the weakness of Albania's institutional capacity. The reforms recommended below assume a judicial infrastructure (training, resources, and appellate oversight) that may exceed Albania's current institutional capacity.

This is a legitimate limitation acknowledged in this paper, and future research should examine implementation challenges specific to jurisdictions in transition.

Positioning of Findings Against SOTA: External Validity and Theoretical Implications

The empirical findings of this study, a 95.6% rate of unauthorized data access, a mean proportionality score of 0.14, and zero recognition of mobile devices as protected correspondence, must be situated within the broader SOTA landscape to assess their

theoretical significance and external validity. Three SOTA benchmarks are employed for this purpose.

First, comparison with [7, 68]. The transatlantic comparative work of Newell and Koops demonstrates that both U.S. post-Riley jurisprudence and European post-ECtHR doctrine converge on a model of layered judicial authorization for smartphone searches. Their analysis treats such authorization as the doctrinal baseline for constitutional compliance in mature democracies. The present study reveals that Albania operates at a structural distance from this baseline: not a distance of degree (e.g., 60% vs. 100% authorization rates) but a distance of category (0% in 153 decisions vs. 100% in the SOTA comparators). This categorical gap is not predicted by [7], whose framework assumes a transitional trajectory toward convergence. Our data suggest that in post-communist legal systems, the trajectory is not automatic: classification inertia and legislative underspecification can produce stable non-convergence even after a decade of EU integration efforts. This is a theoretically significant finding that extends beyond Albania.

Second, comparison with Kerr's mosaic theory [10]. Kerr's mosaic theory predicts that judicial systems will eventually recognize the aggregation problem — the fact that individually innocuous data points, when combined, produce a comprehensive portrait of private life — and adjust procedural safeguards accordingly. The Albanian data empirically test this prediction for the first time in a post-transition context: the prediction is not borne out over an eight-year period (2017–2025), even post-Supreme Court guidance (2021). This constitutes a theoretically meaningful disconfirmation: aggregation awareness in judicial reasoning cannot be assumed to emerge spontaneously from doctrinal development; it requires explicit legislative operationalization. This finding has implications for jurisdictions in similar transitional phases, including other Western Balkan states pursuing EU accession.

Third, comparison with Barak's proportionality framework [12]. Barak's four-stage proportionality model (proper purpose, rational connection, necessity, proportionality stricto sensu) functions in this study as the normative benchmark for the PS scoring instrument. Critically, the mean PS of 0.14 in Albanian decisions corresponds to a near-total failure at Stage 1 (proper purpose, here: classification as correspondence), which structurally blocks all downstream proportionality analysis. This is analytically different from partial proportionality failures documented in ECtHR case law, where Stage 1 is typically satisfied and failures occur at Stages 3 or 4. The Albanian configuration represents a "pre-proportionality" failure mode not addressed in Barak's framework, which assumes baseline constitutional recognition. The PS instrument operationalizes this failure mode for the first time in a dataset of this size, constituting a modest but defensible novel contribution to the empirical application of proportionality theory in digital evidence contexts.

In terms of external validity, the findings are bounded by the Albanian jurisdictional context and the 2017–2025 timeframe. They cannot be directly generalized to other post-communist legal systems without replication. However, the analytical framework — the

combination of PS scoring, classification-based hypothesis testing, and SOTA-anchored benchmarking is fully portable and represents the primary transferable contribution of this study. Jurisdictions with analogous classification problems (material evidence vs. digital correspondence) and comparable institutional development profiles may find the PS instrument a useful diagnostic tool for identifying structural proportionality deficits prior to legislative reform.

SUMMARY AND CONCLUSION

The current research has explored systematically the constitutional, the procedural and the practical field of mobile device data seizure in Albania. Combining the jurisprudential, conceptual and theoretical argument of privacy, correspondence and proportionality [35, 36, 53-55], the empiric data of 160 court decisions [28, 29] and the advanced jurisprudential developments [86–89], the study exposes the discrepancy of the Albanian jurisprudence compared to the international standards, in the application of the mobile device as evidence. The courts in Albania look at the mobile devices practically as physical evidence, ignoring the mobile device as a place of correspondence, and misapplying the proportionality as its doctrine, with only 4.4 proportions of authorizations issued [28, 29], and no recognition of the right to secrecy of correspondence on the constitution [18], with an average proportionality score of 0.14.

This points to the fact that there is a structural discontinuity between how investigations are carried out and how constitutional rights are protected. The Guidelines issued by the Supreme Court in its Unifying Decision No.8493/2021[28] and the decision issued by the Constitutional Court in its Decision No.4487/2025 [29] are the guides by which national practice can be brought more in line with the norms of human rights. Particularly, they relate to narrowly defined contraband, layered authorization from the courts and weight on proportionality approaches to digital evidence. The data collected reveal that the implementation of these safeguards results in a significant climb in the proportionality index and implies that the steady implementation of the various constitutional and procedural values reflected within the Guidelines and the Decision can, over time, lead to the elimination of these gaps [28, 29, 36, 55].

Taken as a whole, the theoretical, empirical, and comparative analysis in this study yields three conclusions of broader significance. First, the “pre-proportionality failure mode” identified here — whereby Stage 1 of Barak’s proportionality model is never reached because courts do not recognize the protected constitutional interest at the outset — represents a structurally distinct category of rights deficit not captured by existing SOTA frameworks, which universally assume baseline constitutional recognition. Second, the data disconfirm Kerr’s implicit convergence assumption: aggregation awareness in judicial reasoning does not emerge automatically from doctrinal exposure over an eight-year period; it requires explicit legislative operationalization. Third, the Proportionality Score (PS) instrument introduced in this study is analytically portable: it can be applied to any jurisdiction facing an analogous classification problem to produce a comparable

diagnostic baseline, making it a transferable methodological contribution beyond the Albanian context. Drawing upon these conclusions, the study offers the following recommendations for policy, practice, and further research:

Applying these principles to digital evidence in the form of mobile devices, considering their use as correspondence, and making law reforms accordingly is necessary. To achieve this point through legislation, reform should explicitly require that mobile device data be recognized as constitutionally protected correspondence pursuant to Article 36 of the Albanian Constitution and Article 8 of the ECHR [18, 20].

Protecting the procedural rights of suspects and defendants by requiring a layered judicial authorization before mobile data may be seized and examined can operationalize proportionality and discrimination, and protect against privacy violations [28, 29, 55].

International standards and the application of principles of proportionality could be incorporated into the training of prosecutors, judges, and law enforcement agents and articulated in manual directives for handling mobile evidence [28, 29, 35, 36]. Proportionality can be incorporated into the operational standards for law enforcement investigations and prosecutions.

Procedural safeguards should include mandatory national guidelines for forensic examination of mobile evidence, including procedures for carriage, storage, imaging, hashing, and documentation of removal, storage, and analysis, as well as for the chain of custody [6, 31, 32, 37].

Training programs for prosecutors, judges, and law enforcement should emphasize the development of interpretations of technological neutrality, theories of privacy, and appropriate forensic techniques including the application of principles of proportionality and knowledge of comparative jurisprudence, state practice, and human rights standards [27, 28, 35, 53, 55].

Monitored measurement of statistics gathering about mobile device seizure frequency, judicial authorizations, and proportionality assessment will facilitate the evaluation of the impact and effectiveness of any recommendations and reform trends and address concentration of investigative authority issues within the CJEU [1,17,55].

Future research should explore the wider context of privacy doctrine, the scope of proportionality, and the introduction of newer emerging technologies, such as cloud storage, with a view toward a comparative model of constitutional convergence with established European standards [4, 37–39].

In conclusion, this study demonstrates that the Albanian legal system operates in a structurally distinct deficit mode with respect to digital evidence — one that is empirically measurable, theoretically explicable through the “pre-proportionality failure” construct, and analytically comparable across jurisdictions via the PS instrument. The Constitutional Court’s Decision No. 44/2025 provides the necessary doctrinal foundation to exit this mode, but the transition from constitutional mandate to measurable judicial practice will require concurrent legislative reform and institutional capacity-building. The PS framework introduced here offers a replicable instrument to monitor this transition empirically in

Albania and to benchmark analogous post-transition legal systems against international human rights standards [28, 29, 35–37, 53–55].

Beyond its local focus, this study offers a theoretical model for assessing digital privacy in transitional democracies. Albania serves as a pertinent case study for how legal systems adapt or fail to adapt to the 'digital-by-default' nature of modern evidence. The 'Proportionality Score' introduced here can be replicated in other jurisdictions to measure the alignment between domestic practices and international human rights benchmarks

AUTHORS CONTRIBUTIONS

Conceptualization, Y.P.; Methodology, Y.P., and F.Z.; Software and Computational Modelling, F.Z.; Validation, Y.P., and F.Z.; Formal Analysis, Y.P., and F.Z.; Investigation, Y.P.; Resources, Y.P.; Data Curation, Y.P., and F.Z.; Writing Original Draft Preparation, Y.P.; Writing – Review & Editing, Y.P., and F.Z.; Visualization, Y.P; Supervision, F.Z.

ACKNOWLEDGMENT

The authors wish to thank sincerely the prosecution and court administrative where the authors obtained the court decisions and legal documentation required as it has been crucial for the empirical and jurisprudential analysis included in the present publication.

CONFLICT OF INTERESTS

The authors hereby declare that there are no conflicts of interest associated with this publication. All findings and interpretations presented are solely those of the author and have not been influenced by any external entity.

REFERENCES

1. Bernardini, L.; Sanvitale, F. Searches and seizures of electronic devices in European criminal proceedings: A new pattern for independent review? *Rev. Ítalo-Española Derecho Procesal* **2023**, *1*, 73–119.
2. Troisi, P. Le investigazioni digitali sotto copertura; Cacucci Editore: Bari, Italy, **2022**.
3. Horsman, G. The importance of digital evidence strategies. *WIREs Forensic Sci.* **2023**, *6*(1), e1507.
4. James, J. E. Foundations of mobile forensics: An academic approach. *Issues Inf. Syst.* **2024**, *25*(3), 94–108.
5. Court of Justice of the European Union. Judgment of the Grand Chamber, Case C-548/21, 4 October 2024. Availble online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0548 (accessed on 27 December 2025).
6. Curran, K., Robinson, A., Peacocke, S., Cassidy, S. Mobile phone forensic analysis. *Int. J. Digit. Crime Forensics* **2010**, *2*(3), 1–13.
7. Newell, B.C., Koops, B.-J. From horseback to the moon and back: Comparative limits on police searches of smartphones upon arrest. *Hastings Law J.* **2020**, *72*(1), 229–290.

8. Stoilkovski, M. Guidelines on Cybercrime Investigation; OSCE Mission in Tirana: Tirana, Albania, **2022**.
9. Hirvelä, P., Heikkilä, S. Right to Respect for Private and Family Life, Home and Correspondence: A Practical Guide to the Article 8 Case Law of the European Court of Human Rights; Intersentia / Cambridge University Press: Cambridge, UK, **2023**.
10. Kerr, O.S. The mosaic theory of the Fourth Amendment. *Mich. Law Rev.* **2012**, *111*(3), 311–354.
11. Nissenbaum, H. Privacy as contextual integrity. *Wash. Law Rev.* **2004**, *79*, 119–158.
12. Barak, A. Proportionality: Constitutional Rights and Their Limitations; Cambridge University Press: Cambridge, UK, **2012**.
13. Solove, D.J. Understanding Privacy; Harvard University Press: Cambridge, MA, USA, **2008**.
14. Horsman, G. A template for creating and sharing ground truth data in digital forensics. *J. Forensic Sci.* **2024**, *69*(4), 1456–1466.
15. Koops, B.J. Should ICT regulation be technology neutral? In Starting Points for ICT Regulation; Koops, B. J., Ed.; TMC Asser Press: The Hague, Netherlands, **2006**; pp. 77–108.
16. Ochnio, A. H. The tangled path from identifying financial assets to cross-border confiscation: Deficiencies in EU asset recovery policy. *Eur. J. Crime Crim. Law Crim. Justice* **2021**, *29*, 218–237.
17. Bottoms, A.E., McClean, S. Mixed method research in criminal justice: The integration of empirical and doctrinal approaches. *J. Crim. Law Criminol.* **2014**, *104*(1), 1–30.
18. Albanian Constitution, 1998 (as amended); Parliament of the Republic of Albania: Tirana, Albania. Available online: http://cec.org.al/Portals/0/Documents/CEC%202013/Albanian%20Constitution.pdf (accessed on 20 September 2025).
19. Criminal Procedure Code of the Republic of Albania, 1995 (as amended); Ministry of Justice: Tirana, Albania. Available online: https://www.drejtesia.gov.al/wp-content/uploads/2025/10/EN-_-ligj-7905-21031995-Kodi-i-Procedures-Penale-perditesuar-2021-ANGLISHT.pdf (accessed on 20 September 2025).
20. European Convention on Human Rights; Council of Europe: Rome, Italy, 1950. Available online: https://www.echr.coe.int (accessed on 20 April 2025).
21. Charter of Fundamental Rights of the European Union; Official Journal of the European Union, C 326, 391–407, 2012. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT (accessed on 05 December 2025).
22. Directive (EU) 2016/680 on the Protection of Personal Data; Official Journal of the European Union, L 119, 89–131, 2016. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 (accessed on 20 September 2025).
23. Kaye, D. H. Privacy in the Age of Digital Evidence: Comparative Trends in Mobile Data Law. *J. Law Policy* **2019**, *45*(2), 123–158.
24. Big Brother Watch and Others v. United Kingdom, App. No. 58170/13, European Court of Human Rights, 13 September 2018. Available online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]} (accessed on 20 September 2025).
25. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Case C-293/12, Court of Justice of the European Union, 8 April 2014. Available online: https://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293 (accessed on 20 September 2025).

26. Carpenter v. United States, 585 U.S. , Supreme Court of the United States, **2018**.
27. Italian Constitutional Court, Judgment No. 262/2014; Corte Costituzionale: Italy, **2014**.
28. Supreme Court of Albania, Unifying Decision No. 147/2021; Tirana, Albania, **2021**.
29. Constitutional Court of Albania, Decision No. 44, 29 July 2025 (V-44/25); Tirana, Albania, **2025**.
30. Levi, M., Osofsky, L. Investigating, seizing and confiscating proceeds of crime. *Crime Law Soc. Change* **2020**, *73*, 1–26.
31. Punja, S., Mislan, R. Mobile Device Analysis. Small Scale Digit. *Device Forensics J.* 2008, *2*(1), 1–16.
32. Jansen, W., Delaitre, A., Moenner, L. Overcoming impediments to cell phone forensics. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 7–10 January 2008; IEEE: Piscataway, NJ, USA, **2008**; pp. 483–483.
33. Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, 4 December 2015. Available online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]} (accessed on 20 September 2025).
34. Koops, B.-J. The trouble with European data protection law. *Int. Data Privacy Law* **2014**, *4*(4), 250–261.
35. Gunuganti, A. Privacy and Data Protection in the Digital Age. *Journal of Scientific and Engineering Research*, **2018**, *5*(12), 358-365.
36. Abdullah, H.O., Maqsood, M., Nadeem, A. Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era. Research Journal for Social Affairs **2025**, *3*, 795-805.
37. Karjagi, S.A., Quadri, R.A., 37. Karjagi, S. Forensic investigation of mobile phones utilizing mobile forensics tools. *Eur. Chem. Bull.* **2023**, *12*(5), 5782–5791.
38. Vinayagam, P.S. Mobile forensics: Investigation and tools. *Int. J. Comput. Trends Technol.* **2025**, *73*(6), 7–15.
39. Riley v. California, 573 U.S. 373, Supreme Court of the United States, **2014**.
40. European Court of Human Rights, Kruglov and Others v. Russia, No. 11264/04, 4 February **2020**.
41. European Court of Human Rights, Vinks and Ribickas v. Latvia, No. 28926/10, 30 January **2020**.
42. Ontario Court of Appeal. R. v. Fearon, 2019 ONCA 130; Ontario, Canada, **2019**.
43. Morić, Z., Dakić, V., Ogrizek Biškupić, I. An Empirical Assessment of Digital Forensic Process Reliability Using Integrated ISO/IEC 27037 and 27041 Standards. *J. Cybersecur. Priv.* **2026**, *6*, 57.
44. Supreme Court of Albania, Penal College, Decision No. 76, 25 March 2024; Tirana, Albania, **2024**.
45. General Prosecution Office of Albania. Annual Reports 2021 and 2022; GPO Publications: Tirana, Albania, **2022**.
46. SPAK – Special Structure Against Corruption and Organised Crime. Annual Reports 2021 to 2025; Online SPAK Publications: Tirana, Albania. Available online: https://spak.gov.al/wp-content/uploads/2025/07/SPAK-Annual-Rep.-2024-Raporti-Vjetor-SPAK-2024.pdf (accessed on 27 December 2025).

47. General Prosecution Office of Albania. Archival Criminal Case Files – Tirana, Lezhë, Shkodër; Internal Documentation. Available online: https://www.pp.gov.al/Prokuroria_e_Pergjithshme_en/ (accessed on 27 December 2025).
48. Interviews conducted with a prosecutor and a judge in Albania, October **2024**.
49. Berring, R. C. Legal Information and the Search for Cognitive Authority. *UC Berkeley Public Law and Legal Theory Working Paper No. 99-1.* **1999**, 1–26.
50. Garner, B.A. Black's Law Dictionary, 10th ed.; Thomson Reuters: St. Paul, MN, USA, **2016**.
51. Zweigert, K.; Kötz, H. An introduction to comparative law; Oxford University Press: Oxford, UK, **1998**.
52. Reimann, M. Comparative law: European and global perspectives; Kluwer Law International: The Hague, Netherlands, **2005**.
53. Alexy, R. A theory of constitutional rights; Oxford University Press: Oxford, UK, **1985**.
54. Alexy, R. Constitutional rights, balancing, and rationality. *Ratio Juris* **2002**, *16*(2), 131–140.
55. Cohen-Eliya, M., Porat, I. Proportionality and constitutional culture; Cambridge University Press: Cambridge, UK, **2013**.
56. Brownsword, R., Yeung, K. Regulating technologies: Legal futures, regulatory frames and technological fixes; Hart Publishing: Oxford, UK, **2008**.
57. Dyzenhaus, D. The constitution of law: Legality in a time of emergency; Cambridge University Press: Cambridge, UK, **2009**.
58. Branislav Kotrč "Mobile big data architecture", Master's Thesis, Masaryk University Faculty of Informatics, Brno, Spring **2021**.
59. Natarajasivan, D., Govindarajan, M. An Overview on mobile data mining", *International Journal of Computer Applications*. **2014**, *99*, pp. 11–14.
60. Dedić, N., Stanier, C. Towards Differentiating Business Intelligence, Big Data, Data Analytics and Knowledge Discovery. *Lecture Notes in Business Information Processing*. **2017**; pp. 114–122.
61. Thabet, N., & Soomro, T.R.. Big Data Challenges. *Journal of Computer Engineering & Information Technology*. **2015**, *4*, 1000133
62. C. Dizon, M. A., & Meehan, A. Technical principles and protocols of encryption and their significance and effects on technology regulation. *Information & Communications Technology Law* **2025**, *34*(2), 79–105.
63. Marco Kühnel "Encryption from a Human Rights Perspective". Available online: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/MarcoKuhnel.pdf (accessed on 27 December 2025).
64. Maniadaki, M., Alexakis, D.D., Maria, E.-A. Use of Drones in Disasters in the European Union: Privacy Issues and Lessons Learned from the COVID-19 Pandemic and Mass Surveillance Jurisprudence of the ECtHR and the CJEU. *Laws* **2025**, *14*, 27.
65. Constitutional Court of Italy. Decision No. 170, 27 July 2023 (data ud. 07 June 2023). Available online: https://canestrinilex.com/en/readings/electronic-messages-are-protected-correspondence-constitutional-court-17023 (accessed on 28 December 2025).
66. Constitutional Court of Austria. VfGH-Erkenntnis G-352-2021, 14 December 2023. Avilable online: https://www.vfgh.gv.at/downloads/VfGH-Erkenntnis-G_352_2021-46-vom-14.12.2023-EN.pdf (accessed on 28 December 2025).

67. European Court of Human Rights. Saber v. Norway, Application No. 459/18, 17 March 2021. Available online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-206519%22]} (accessed on 29 December 2025).
68. Newell, B.C., Koops, B.-J. Privacy and Security in Smartphone Searches: A Transatlantic Perspective. *Crim. Justice Ethics* **2020**, *39*(1), 1–23.
69. Stoilkovski, G. *Cybercrime Investigation and Digital Evidence: OSCE Guidelines and Practice.* OSCE Publ. **2022**.
70. Karagiannis, C., Vergidis, K. Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information* **2021**, *12*, 181.
71. FRA. European Convention on Human Rights - Article 8. Available online: https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0 accessed on 29 December 2025).
72. Solove, D.J. A Taxonomy of Privacy. *Univ. Pa. Law Rev.* **2006**, *154*(3), 477–560.