



Research Article

© 2026 Renis Sheshi

This is an open access article licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (<https://creativecommons.org/licenses/by-nc/4.0/>)

Open-Source Intelligence and the Right to a Fair Trial: Balancing Investigative Efficiency with Procedural Guarantees

PhD (C.) Renis Sheshi

“Barleti” University, Tirana, Albania

DOI: <https://doi.org/10.2478/bjir-2026-0012>

Abstract

Open-source intelligence (OSINT) has become a dominant investigative methodology of Western law enforcement, yet the procedural frameworks governing its use as courtroom evidence remain underdeveloped. This article examines whether the fair trial guarantees under Article 6 of the European Convention on Human Rights, equality of arms, adversarial proceedings, and the reasoned judicial evaluation of evidence, are adequate to the specific challenges OSINT presents.

Drawing on the jurisprudence of the European Court of Human Rights, the article argues that the existing guarantees are doctrinally adequate to this task, and identifies the specific requirements that follow from their application to evidence of open-source origin. A comparative analysis of the United Kingdom and the Netherlands shows how two established jurisdictions handle the intelligence-to-evidence transition differently, and why neither approach has yet been translated into a procedural regime adequate to the particular features of OSINT. The Western Balkans, and Albania in particular, illustrate what follows when investigative capability is expanded through international capacity-building programmes while procedural safeguards in this specific area remain largely undeveloped. The article identifies three implications of Article 6 that domestic criminal justice systems must observe when OSINT evidence is relied upon at trial: disclosure of methodology, preservation of the material in forensically sound form at the point of collection, and defence access to the underlying data in conditions that permit independent verification. These implications are doctrinal rather than novel, and the task for domestic legislators and courts is to give them practical effect before investigative practice becomes entrenched.

Keywords: Open-source intelligence (OSINT); right to a fair trial; Article 6 ECHR; intelligence-to-evidence transition; Albania.

1. Introduction

Criminal procedure has consistently struggled to keep pace with the investigative tools available to law enforcement, and open-source intelligence (OSINT) is a prominent example of this gap. OSINT is commonly defined as the systematic collection, processing, and analysis of information derived from publicly accessible sources. By some estimates, it now accounts for between 80% and 90% of intelligence activity conducted by Western law enforcement agencies (Ghioni et al., 2024). Social media posts, commercial satellite imagery, publicly filed corporate records, blockchain transaction logs, cached web pages, and geolocated photographs are no longer merely supplementary leads; rather, they increasingly constitute the evidentiary backbone of criminal prosecutions. The procedural architecture designed to ensure fairness in criminal proceedings—developed through decades of European Court of Human Rights (ECtHR) jurisprudence—was originally conceived for a legal environment in which evidence possessed relatively stable material forms, such as documents, recordings, or physical objects. Investigative practice has since evolved into a domain in which evidence may be altered, manipulated, or deleted at any moment, and in which the processes of collection and analysis are often opaque to all but the investigating authorities.

In the Grand Chamber judgment of *Yüksel Yalçınkaya v. Türkiye* (2023), the ECtHR addressed this tension directly, finding a violation of Article 6 § 1 of the European Convention on Human Rights where the applicant's conviction was based on encrypted messaging data that he could neither access nor meaningfully challenge. The Court held that digital evidence must be subject to adversarial scrutiny and that domestic courts must independently assess its integrity rather than defer to the assertions of intelligence agencies or technical experts. The judgment further identified the issue as systemic under Article 46, noting that more than 8,000 similar applications were pending before the Court. This illustrates how deficiencies in the procedural handling of digital evidence can generate large-scale human rights implications. A review of the relevant academic literature indicates that the relationship between OSINT methodologies and Article 6 ECHR fair trial guarantees remains largely underexplored. Stoykova (2023) comes closest to addressing this intersection; however, her analysis focuses on digital evidence in general rather than OSINT specifically and does not extend to the Western Balkans or Albania, where such techniques are increasingly adopted without corresponding procedural development. This article addresses this gap by examining the intersection of OSINT and fair trial guarantees. It argues that the procedural safeguards embedded in Article 6 are, in principle, sufficient to regulate the use of OSINT-derived evidence at trial, provided that their practical implications for this category of evidence are properly identified and applied. At present, however, these implications remain largely underdeveloped in domestic procedural frameworks. The analysis that follows is primarily doctrinal. It relies on a close reading of ECtHR jurisprudence concerning digital evidence and Article 6 guarantees in order to identify the procedural requirements applicable to OSINT-derived material.

This doctrinal core is supplemented by a comparative analysis of two jurisdictions, the United Kingdom and the Netherlands selected as representative of common law and civil law traditions, respectively. The comparison is not intended to be exhaustive; rather, it serves to illustrate how two established legal systems have addressed the transition from intelligence gathering to evidentiary use, and to identify unresolved issues within each framework. The findings are subsequently applied to the Western Balkans, with particular focus on Albania, in order to assess the region's procedural readiness for the evidentiary use of OSINT. This final step is informed by the author's professional experience within the Albanian judiciary, which provides contextual insight into the practical application of the Code of Criminal Procedure alongside its formal provisions, but is treated solely as contextual background rather than independent empirical evidence. The sources consulted throughout include legal scholarship, primary case law, statutory instruments, and publicly available reports from international capacity-building programmes operating in the region.

2. Defining OSINT in the Criminal Investigation Context

At its broadest, open-source intelligence (OSINT) refers to the collection and analysis of information that is publicly available; that is, information that any member of the public could, in principle, access without recourse to covert methods or special authorisation. Böhm and Lolagar (2021) provide a useful classification that includes both the intended targets (across seven categories) and the principal OSINT tools, such as social media monitoring, web scraping, analysis of publicly accessible databases, and geospatial intelligence derived from commercial satellite imagery. Bazzell (2023) extends this taxonomy by cataloguing more advanced techniques, including the identification of pseudonymous accounts, tracing digital footprints across platforms, exploiting cached and archived web content, and reconstructing deleted material through residual metadata.

OSINT is distinguished from other forms of digital investigation less by the nature of the information itself than by the manner in which it is acquired. Unlike evidence obtained through search warrants, wiretaps, or compulsory production orders, OSINT is gathered from sources that the data subject has voluntarily made available to an unrestricted audience. This accessibility often generates a misleading inference: that because information is publicly available, its collection by state authorities raises no human rights concerns. The European Court of Human Rights has consistently rejected this assumption. In *Benedik v. Slovenia*, the Court held that police access to subscriber information linked to a dynamic IP address engaged Article 8 of the European Convention on Human Rights and required a clear legal basis accompanied by adequate safeguards. The Court further rejected the domestic finding that the applicant had waived his privacy rights by disclosing his IP address in a peer-to-peer environment. While OSINT originates as an intelligence product, its nature changes fundamentally when introduced into judicial proceedings as evidence, as it must then comply with a distinct and more demanding procedural framework. Intel-

ligence is forward-looking, probabilistic, and tolerant of uncertainty; it is primarily used to orient investigative resources and generate hypotheses. Evidence, by contrast, is retrospective, adversarial, and subject to strict procedural safeguards derived from the right to a fair trial. In practice, however, the boundary between these two functions can become blurred to the point of near dissolution. For example, when a police analyst scrapes a suspect's publicly accessible social media profile, the same act simultaneously produces an intelligence product and generates material that may later be introduced as evidence. The same data, collected by the same officer, at the same moment, may thus occupy both categories depending entirely on its subsequent procedural deployment. This dual-use character underscores both the limitations of existing safeguards and the increasing importance of adapting procedural guarantees to OSINT-based investigations.

3. The Intelligence-to-Evidence Transition

Sampson (2016) addresses the question of whether, and under what conditions, open-source intelligence (OSINT) may cross the threshold from intelligence into admissible evidence in criminal proceedings within jurisdictions bound by the European Convention on Human Rights (ECHR). He identifies a set of evidentiary and procedural hurdles that such material must satisfy. These derive both from general principles of the law of evidence and from Article 6 of the ECHR. In particular, the material must be relevant to a fact in issue, reliable in the technical evidentiary sense, and produced through a procedurally sound process. Additional fairness considerations arise, including the lawfulness of the means of acquisition, disclosure obligations of the prosecution, the defendant's right to examine the originator of the evidence, access to adequate facilities for challenge, and compliance with rules governing hearsay. Sampson's central argument is that intelligence and evidence are conceptually distinct categories, and that OSINT, when introduced in court, must satisfy the same forensic and procedural standards as any other evidentiary material.

Authentication presents particular difficulties in this context. A screenshot of a social media post, absent corroborating metadata, establishes only that a specific image existed on a particular screen at a particular time. It does not establish authorship, integrity, or contextual fidelity. Mason and Seng (2021) identify a common law "presumption that computers are reliable," under which courts, absent contrary evidence, assume proper functioning of computer systems at the material time. However, they demonstrate that this presumption is empirically fragile, as illustrated by the Post Office Horizon litigation. Ladkin et al. (2020) reinforce this critique from a software engineering perspective, showing that the Law Commission's presumption does not reflect the operational reality of software systems. Non-trivial software inevitably contains latent defects, many of which manifest infrequently, such that prior error-free operation provides limited assurance of reliability in a specific instance. The authors further conclude that even prior apparent reliability does not justify a presumption of correctness, and that evidence of past failure undermines any such assumption.

These observations have direct implications for OSINT tools, which themselves constitute complex software systems, often no less intricate than transaction-processing platforms already scrutinised by domestic courts. Accordingly, outputs generated by OSINT systems cannot be presumed reliable and must instead be subjected to rigorous evidentiary verification before being accepted as fact. Chain of custody raises further concerns. OSINT is derived from environments over which neither prosecution nor defence exercises control. Social media platforms may alter algorithms, modify interfaces, delete accounts, or change data retention policies without notice. Similarly, user-generated content may be edited, removed, or manipulated by third parties at any time. This inherent volatility undermines the stability of the evidential object. Lagerwaard (2023), in his study of the Dutch Financial Intelligence Unit, illustrates how transaction data collected by private entities are transformed into intelligence and disseminated to investigative and prosecutorial authorities without judicial authorisation or suspect notification. He further notes that the extent to which such intelligence is subsequently relied upon in criminal proceedings remains empirically unclear, highlighting a significant gap in transparency and accountability. His analysis underscores the critical transition point at which intelligence becomes evidentiary material, thereby triggering the procedural safeguards required under fair trial guarantees.

The problematic nature of OSINT as evidentiary material does not imply that it is inadmissible *per se*; rather, it necessitates robust procedural frameworks capable of addressing its inherent deficiencies. The most comprehensive articulation of such a framework is provided by the Berkeley Protocol on Digital Open-Source Investigations, jointly issued in 2022 by the Office of the United Nations High Commissioner for Human Rights and the Human Rights Center at the University of California, Berkeley. The Protocol establishes professional standards for the identification, collection, preservation, analysis, and presentation of digital open-source information, structured around three tiers: professional principles (including accountability, competence, objectivity, legality, and security awareness), methodological principles (including accuracy, data minimisation, preservation, and security by design), and ethical principles (including dignity, humility, inclusivity, independence, and transparency). It further outlines a six-phase investigative cycle comprising online inquiry, preliminary assessment, collection, preservation, verification, and analysis (Berkeley Protocol, 2022, §§ 24–38, 140).

Verification, which is central to judicial assessment of OSINT material, is further divided into three components: source analysis (provenance, credibility, independence, and specificity), technical analysis (metadata, exchangeable image file format data, and source code integrity), and content analysis (including geolocation, chronolocation, internal consistency, and external corroboration) (Berkeley Protocol, 2022, §§ 176–194). Although designed primarily for international criminal and human rights investigations, these criteria reflect an underlying logic of evidentiary assessment that is readily transferable to domestic criminal proceedings, where courts are required to assess relevance, probative value, and the balance between probative value and prejudicial impact under fair trial guarantees (Berkeley Protocol, 2022, § 56).

4. OSINT Specific Tensions with Procedural Rights

The challenges surveyed above apply to digital evidence generally. However, open-source intelligence (OSINT) introduces an additional and distinctive set of concerns arising from its specific mode of intelligence collection, its relationship to the data subject, and the interpretive processes through which raw open-source information is transformed into a prosecutorial narrative. Replicability represents one of the clearest points of divergence between OSINT and conventional forensic evidence. In traditional forensic practice, a central safeguard lies in the defence's ability to independently examine and, where necessary, re-test evidential material—for example, by re-testing DNA samples, re-examining crime scene photographs, or commissioning independent ballistic analysis. In the context of OSINT, such replicability is often unattainable. Social media content may be deleted, web pages may be altered, user profiles may be modified, and platform algorithms may restructure the informational environment in which the original data existed. As a result, the defence cannot retrospectively replicate the investigator's act of collection. Where material has not been preserved in a forensically sound manner at the time of acquisition, the opportunity for meaningful verification is permanently lost.

A further challenge arises from algorithmic intermediation. Contemporary OSINT practice increasingly relies on automated or semi-automated tools, including web scraping software, facial recognition systems, natural language processing models, and network analysis platforms. These tools enable analysis at a scale beyond human capability, yet the processes by which they generate outputs are often opaque. Quattrocolo, Anglano, Canonico, and Guazzone (2020) identify this as a fundamental evidentiary problem: outputs produced by advanced mobile forensic platforms frequently fail to disclose how information has been extracted from underlying data, thereby preventing meaningful assessment of completeness or accuracy without independent forensic reconstruction requiring both legal and computational expertise. Galič (2021) identifies a related structural asymmetry in the context of the principle of equality of arms under Article 6 ECHR. Drawing on Strasbourg jurisprudence and the Dutch experience with the Netherlands Forensic Institute's Hansken platform, he demonstrates that advanced forensic systems may confer a systemic advantage on the prosecution that cannot be remedied merely by granting the defence additional preparation time. Time alone is insufficient where the defence lacks equivalent access to the underlying tools, and therefore cannot effectively test the reliability of the evidential outputs or assess whether alternative queries would have produced exculpatory results.

OSINT also introduces risks associated with pre-trial narrative construction through digital profiling. Sachoulidou (2024) argues that algorithmic profiling effectively raises an "innocence threshold," requiring individuals to rebut a pre-existing narrative constructed from their digital traces before formal proceedings even commence. OSINT-based suspect identification can be understood as a form of algorithmic pro-

filing, thereby engaging these concerns directly. De Hert and Gutwirth (2006) similarly argue that the processing of personal data is inherently embedded within relations of power, as data collection not only reflects but also shapes behaviour and enables forms of control that may remain invisible to the data subject. Within their framework, profiling is situated among practices that may require prohibitive rather than merely procedural regulation, given that large-scale data aggregation can produce concentrations of power that undermine the opacity function traditionally served by privacy protection. They further caution that when data protection regimes operate primarily through procedural “channelling,” they risk implicitly legitimising emerging forms of power that may not yet have been normatively justified.

5. ECtHR Case Law on Digital Evidence and Adversarial Scrutiny

These tensions find only partial and indirect resolution in the Strasbourg case law. Although no judgment addresses open-source intelligence (OSINT) explicitly, two interrelated strands of authority establish the relevant principles: one concerning adversarial scrutiny of digital evidence, and the other concerning the safeguards required when the state engages in large-scale digital information collection.

In *Yüksel Yalçınkaya v. Türkiye* (2023), the Grand Chamber found violations of Articles 6 § 1, 7, and 11 of the European Convention on Human Rights where the applicant’s conviction for membership in a terrorist organisation was based decisively on data derived from the ByLock encrypted messaging application. The applicant had no meaningful access to this data and was unable to examine or effectively challenge it. The Court held that digital evidence must be subject to genuine adversarial scrutiny and that domestic courts cannot merely endorse findings produced by intelligence or law-enforcement authorities. Instead, they are required to engage substantively with defence challenges concerning authenticity and integrity and to ensure that the defence has a real opportunity to subject such material to independent expert examination. The Court further characterised the underlying issue as systemic under Article 46, noting that more than 8,000 similar applications were pending before it and that Turkish authorities had identified approximately 100,000 ByLock users. This scale illustrates how procedural deficiencies in the handling of digital evidence can produce systemic human rights consequences. The reasoning extends naturally to OSINT-derived material: where the defence lacks access to underlying data, cannot interrogate collection methodologies, and is unable to test the reliability of analytical tools, the requirements of Article 6 are not satisfied.

The Grand Chamber judgments in *Big Brother Watch and Others v. the United Kingdom* (2021) and *Centrum för Rättvisa v. Sweden* (2021) established the “end-to-end safeguards” framework for bulk interception regimes. This requires that safeguards operate at every stage of the surveillance process, including prior independent authorisation, supervision of selection criteria (bearers and selectors), and oversight of the use, storage, transfer, and destruction of intercepted material. Although developed in the context of communications surveillance, the underlying principle that

legal safeguards must apply across the entire evidential lifecycle—has clear relevance for OSINT practices, which similarly involve multi-stage data collection and processing chains.

In *Benedik v. Slovenia* (2018), the Court held that police acquisition of subscriber information linked to a dynamic IP address engaged Article 8 and required a clear legal basis accompanied by adequate safeguards, notwithstanding that such data were technically accessible through internet service providers. The Court rejected the assumption that public technical accessibility eliminates Convention protection. Applied to OSINT, this reasoning confirms that the mere availability of information on the open internet does not, in itself, exempt its collection, retention, or use from Article 8 scrutiny.

Similarly, *Roman Zakharov v. Russia* (2015) articulated minimum “quality of law” requirements for communications surveillance, emphasising that legal frameworks must be sufficiently clear, foreseeable, and capable of preventing arbitrary interference. When applied to OSINT, these requirements expose a significant regulatory gap: in many jurisdictions, the legal basis for systematic state collection of open-source digital data is either absent, insufficiently precise, or dispersed across legal instruments not designed to regulate such practices. This lack of normative clarity corresponds directly to the deficiencies identified in *Zakharov* as incompatible with the rule of law.

In *Bărbulescu v. Romania* (2017), the Grand Chamber developed six proportionality criteria in the specific context of employer monitoring of employee communications under Article 8. While confined to that employment setting, the judgment nonetheless reflects a broader principle: that the assessment of digital evidence depends not only on its use at trial but also on the conditions under which it was obtained and processed. In *López Ribalda and Others v. Spain* (2019), concerning covert video surveillance in an employment dispute, the Court held that such evidence did not, in itself, violate Article 6 § 1, provided that the applicants had a genuine opportunity to challenge its authenticity and probative value and that it was not the sole basis for the domestic courts’ findings.

Taken together, these judgments indicate an emerging Strasbourg approach that evaluates fairness holistically. This approach increasingly encompasses not only the evidential use of material at trial, but also the legality, transparency, and contestability of the processes through which such material is obtained and transformed into evidence.

6. Fair Trial Guarantees Under Article 6 ECHR and Their Application to Digital Evidence

The practical implications of this case law for digital evidence have been developed primarily in recent scholarship. Article 6 of the European Convention on Human Rights was originally framed with evidentiary material of relatively stable material form in mind, and its application to open-source intelligence (OSINT) exposes con-

ceptual and procedural gaps that recent literature has only begun to address. Stoykova's body of work represents a sustained effort to derive evidentiary rules for digital investigations from this jurisprudential framework. In her 2023 analysis of Article 6 case law, she identifies two clusters of fair trial guarantees applicable to digital evidence: those grounded in equality of arms and those grounded in the presumption of innocence. She demonstrates that both clusters generate obligations that extend backwards from the trial stage into the investigative phase. While this framework addresses digital evidence in general terms rather than OSINT specifically, it nonetheless provides the doctrinal foundation upon which any OSINT-specific extension must build.

In earlier work, Stoykova (2021) identifies three categories of unaddressed risks arising in technology-assisted investigations: the inconsistent and inappropriate use of investigative technologies, the persistence of outdated procedural safeguards ill-suited to contemporary digital evidence practices, and the absence of systematic reliability testing in digital forensic methods. She argues that these deficiencies necessitate legislative intervention and the introduction of validation standards in order to preserve the presumption of innocence. In her most recent contribution, Stoykova (2024) advances the concept of a "right to procedural accuracy" under Article 6. This proposed right encompasses protection against unreliable digital evidence processing, access to the chain of evidence accompanied by explanation and forensic assistance, and participation in determinative stages of digital evidence production. Across this trajectory, her work progresses from diagnosis (2021), to doctrinal mapping of fair trial obligations (2023), to normative proposal (2024).

Custers (2024) shifts attention from doctrinal development to judicial capacity, arguing that Article 6 ECHR implies a requirement that judges possess sufficient technological literacy to evaluate complex digital processes, and that the absence of such understanding undermines the fairness of proceedings. His analysis of the Amsterdam Uber litigation is particularly illustrative. At first instance, the Court of Amsterdam accepted Uber's representations regarding its systems without substantive scrutiny. On appeal, however, the Court of Appeal overturned this approach, holding that the data controller bore an enhanced duty to justify any refusal of transparency, given its exclusive control over the relevant information. This divergence demonstrates how asymmetries of technical knowledge and informational control between litigants and the court can render Article 6 guarantees ineffective in practice where adjudication depends on complex digital systems.

Although developed in the context of data protection, Custers' reasoning is directly relevant to OSINT evidence, the probative value of which often depends on technical and contextual factors such as platform moderation policies, data ephemerality, potential manipulation or fabrication, and the reliability of geolocation metadata. Each of these elements requires specialised technical understanding that may exceed the capacity of traditional judicial assessment without expert support.

De Hert and Gutwirth (2006) situate these procedural concerns within a broader constitutional theory of the European Convention system. They distinguish between "opacity tools," such as the right to privacy under Article 8, which impose substan-

tive limits on state interference, and “transparency tools,” such as data protection and criminal procedure, which regulate and structure the exercise of legitimate state power. They argue that the European Court of Human Rights has progressively merged the procedural guarantees of Articles 6 and 13 into the legality analysis under Article 8, thereby weakening the independent normative force of each provision. Article 13, in particular, has been rendered largely subsidiary to Article 8 analysis, while Article 8 itself has increasingly incorporated procedural considerations traditionally associated with Articles 6 and 13.

According to De Hert and Gutwirth, this conceptual convergence risks diluting the distinct constitutional functions of these provisions. Their insistence on maintaining a clear separation between opacity and transparency tools has important implications for OSINT in criminal proceedings. Preserving this distinction restores Article 6 to its autonomous role as a guarantor of fair trial rights, including adversarial scrutiny of evidence, equality of arms, and reasoned judicial assessment of reliability. At the same time, Article 8 retains its proper function as the provision governing the substantive legality of state interference in the collection of personal data. Read together, these provisions establish a dual requirement: OSINT must be gathered within the substantive limits imposed by the right to privacy, and it must subsequently be processed and assessed in accordance with the procedural safeguards of a fair trial.

7. Comparative Perspectives: The United Kingdom and the Netherlands

The United Kingdom and the Netherlands adopt markedly different approaches to the treatment of OSINT-derived evidence, and both systems exhibit notable strengths alongside significant procedural gaps. In the United Kingdom, OSINT operates within a fragmented regulatory landscape. Wells and Gibson (2017) document the uneasy coexistence between the Regulation of Investigatory Powers Act (RIPA) framework and the National Police Chiefs’ Council’s five-tier OSINT classification system, which ranges from overt online research to covert online investigative activity. They further note that RIPA predates the expansion of social media and therefore does not sit comfortably with contemporary forms of online investigation. In practice, the legal and procedural requirements applicable to OSINT operations depend heavily on their classification within this administrative hierarchy. Levels 4 and 5 typically require full directed surveillance authorisation, whereas lower tiers are subject to comparatively limited formal oversight. The resulting framework is operationally detailed but legally under-specified, with boundaries that, as Wells and Gibson observe, may have been deliberately left ambiguous.

Sampson (2016; 2017) approaches the issue from a different perspective, emphasizing the conceptual distinction between intelligence and evidence. He argues that OSINT must satisfy ordinary evidentiary thresholds—relevance, reliability, provenance, fairness, hearsay rules, and Article 6 ECHR disclosure obligations—before it can be admitted at trial. Material that is lawfully obtained for intelligence purposes does not automatically acquire evidential status, and where provenance is weak, its probative value before the court is correspondingly reduced.

By contrast, the Netherlands has developed a more formalised regulatory structure, albeit one marked by internal fragmentation. Custers and Stevens (2021) demonstrate that digital data typically enters Dutch criminal proceedings through existing evidentiary categories under Article 339 of the Dutch Code of Criminal Procedure (CCP), most commonly in the form of written police reports. However, the collection of such data is governed by the CCP, while subsequent processing and analysis fall under the Police Data Act and the Justice and Prosecution Data Act. These frameworks are not fully integrated, and automated data analysis in particular remains largely outside a coherent regulatory regime. Moreover, unlawfully obtained evidence rarely leads to exclusion in Dutch courts, given the restrictive interpretation of Article 359a CCP. Lagerwaard (2023) further illustrates the complexity of the Dutch system through his analysis of the Financial Intelligence Unit (FIU). He describes a source-based operational model in which unusual transaction reports submitted by approximately twenty-five categories of reporting entities are aggregated into a restricted-access database. These data are then cross-referenced against police, intelligence, tax, and international datasets using both automated and manual processes. Once designated as suspicious by the Head of the FIU, the information is transferred into a separate dataset accessible to investigative and prosecutorial authorities via the BlueView police system, as well as to foreign partner agencies. Throughout this process, raw transactional data are progressively transformed into financial intelligence through analytical enrichment combining open- and closed-source material. However, the downstream evidential use of this material remains difficult to trace. Importantly, the entire process occurs without judicial authorisation or prosecutorial supervision, and individuals are not notified, as they are not formally designated as suspects. This raises significant concerns regarding the ability of the defence to meaningfully scrutinise material that ultimately enters the criminal case file after undergoing multiple stages of transformation outside the procedural safeguards of criminal proceedings. Galić (2021) examines the structural asymmetries created by advanced forensic tools such as the Netherlands Forensic Institute's Hansken system. He proposes enhanced defence rights, including access to secondary datasets and the search interface itself, the ability to review logs of prosecutorial queries, and the right to commission independent counter-expertise on algorithmic systems. Aksamitowska (2021), in her comparative study of digital evidence practices across Germany, Finland, Sweden, and the Netherlands, similarly highlights the central role of expert intermediaries in judicial interpretation of digital material. These include expertise in cultural and religious context, shadow analysis, voice comparison, and authenticity assessments expressed through probabilistic or likelihood-based scales. While such mediation assists judicial comprehension, it also introduces an additional interpretive layer between raw data and judicial assessment, raising questions about transparency, reliability, and the defence's ability to effectively challenge the evidential basis. Both jurisdictions thus confront a shared structural challenge: the technical capacity for OSINT collection and processing has developed more rapidly than the legal frameworks designed to regulate it. The United Kingdom has responded primarily

through administrative classification and operational guidance rather than statutory reform. The Netherlands, by contrast, has developed a more formal evidentiary architecture, but one largely designed for traditional data sources and not systematically adapted to the distinctive characteristics of OSINT. Neither system has yet developed a procedural framework fully adequate to address the specific challenges OSINT poses under Article 6 ECHR.

8. Implications for Albania and the Regional Context

Countries in the Western Balkans, Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, and Kosovo are at varying stages of the European Union accession process and have all undertaken criminal justice reforms that include the adoption of digital investigative techniques, often with direct international support.

The United States Department of Justice's Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) programme has provided technical assistance to prosecutors across the region, including support for the collection, analysis, and presentation of digital evidence in criminal proceedings (U.S. Department of Justice, n.d.). Eurojust's Western Balkans Criminal Justice Project has likewise organised capacity-building initiatives on digital evidence admissibility, including specialised seminars on encrypted communications evidence and cross-border cooperation (Eurojust, 2023–2025). In addition, the Council of Europe's Second Additional Protocol to the Budapest Convention on Cybercrime (2022) establishes procedural mechanisms for cross-border access to electronic evidence that are directly relevant to these jurisdictions.

These initiatives primarily enhance operational capacity for the use of open-source intelligence (OSINT) and other digital investigative tools, while leaving the underlying procedural infrastructure largely unchanged. Albania illustrates this asymmetry particularly clearly. The Albanian Code of Criminal Procedure contains the structural features typical of a continental evidentiary system: a general definition of evidence in Article 149, a prohibition on the use of unlawfully obtained evidence in Article 151(3), and the principle of free judicial evaluation in Article 152, coupled with an obligation on courts to provide reasoned decisions.

Article 149(2), as amended by Law No. 35/2017 and read in conjunction with Article 8/a, permits courts to admit any item of evidence not expressly regulated by law, provided that it is capable of establishing relevant facts and does not infringe the person's freedom of will, subject to judicial assessment after hearing the parties on the manner of acquisition. This provision constitutes the primary legal gateway through which OSINT-derived material is likely to enter Albanian criminal proceedings. However, it does not establish specific requirements concerning reliability, methodological transparency, authentication, or chain of custody, leaving the assessment of admissibility largely to judicial discretion.

A more specific regulatory framework exists for certain categories of digital evidence. Articles 191/a, 208/a, 299/a, and 299/b of the Code—introduced by Law No. 10054 of 29 December 2008 in implementation of the Budapest Convention—govern the pro-

duction of computer data, seizure of computer systems, and expedited preservation of stored and traffic data. These provisions are significant but limited in scope. Article 191/a applies to offences “in the field of information technology,” while Articles 208/a and 299/a–b apply to offences “related to information technology.” OSINT evidence, however, is most frequently relevant in investigations involving organised crime, corruption, money laundering, and other offences that fall outside these categories. As a result, its use is governed not by the specialised digital-evidence regime, but by the general provisions of Title IV and the residual clause of Article 149(2). The Law on Electronic Documents (Law No. 10273/2010) does not resolve this gap. Although Article 12 provides that electronic documents meeting the criteria of Article 6 may be used as evidence, and requires their validity to be assessed with reference to their creation, storage, transmission, security, and the authenticity of electronic signatures or seals, the law is primarily designed for electronic documents generated in ordinary legal and commercial transactions. It does not establish procedural rules for criminal proceedings, nor does it provide a framework for the evaluation of open-source material or the safeguards required under Article 6 ECHR when such material is relied upon at trial. The practical consequences of this regulatory gap are already observable. Many high-profile criminal proceedings in Albania, particularly those conducted by the Special Anti-Corruption Structure (SPAK), involve complex financial and organised crime investigations in which OSINT could play an increasingly significant evidentiary role. In the author’s professional experience, however, Albanian courts remain insufficiently equipped to assess complex digital evidence, while the defence lacks access to the same level of technical training and expertise that is increasingly available to prosecutorial authorities through international capacity-building programmes. The result is an emerging structural asymmetry in which investigative capabilities are systematically enhanced, while judicial and defence capacities to scrutinise and challenge digital evidence remain comparatively underdeveloped. If this imbalance is to be addressed, the criminal procedure codes of the region will require targeted reform to explicitly regulate OSINT-derived evidence. Such reform could include extending existing digital-evidence provisions beyond cyber-specific offences, introducing mandatory disclosure obligations relating to methodologies and analytical tools, requiring forensically sound preservation at the point of collection, and guaranteeing defence access to underlying data in a form that permits independent verification. The current reform window in Albania and the wider region thus represents a critical opportunity to establish appropriate procedural safeguards before investigative practices become fully entrenched.

9. Applying Existing Fair Trial Guarantees to OSINT Evidence

The preceding parts of this article have documented a set of tensions rather than provided a solution. Investigative capacity in the open-source domain has expanded at a pace that procedural law has not matched. OSINT evidence resists replication in the manner that conventional forensic evidence allows, depends on algorithmic interme-

diation that is frequently opaque even to the analysts who employ it, and enters the courtroom through an evidentiary object that is inherently unstable. Strasbourg has begun to confront these tensions. *Yalçinkaya* is the clearest illustration, but the same concerns surface in *Big Brother Watch*, in *Zakharov*, and in *Benedik*. Taken together, these judgments suggest that the Court is willing to scrutinise not only the use of digital evidence at trial but the conditions under which it was obtained and the extent to which it can be meaningfully contested.

What follows from this is not a call for a new conceptual apparatus. The guarantees contained in Article 6, properly applied, already provide the resources needed to address the specific challenges OSINT presents. The task is to identify what those guarantees require of domestic criminal justice systems when the evidence before the court is open-source in origin, and to insist that those requirements be observed in practice. Three such requirements deserve particular emphasis.

The first concerns disclosure of methodology. The prosecution's duty of disclosure, as developed in *Rowe and Davis v. the United Kingdom* and *Edwards and Lewis v. the United Kingdom* and reiterated in the subsequent case law, extends to material relevant to the defence's capacity to test the evidence against it. Where the prosecution relies on OSINT, the defence cannot test that evidence without knowing how it was produced. The tools employed, the search parameters applied, the platforms consulted, the dates of collection, and the preservation methods used are not collateral information; they are constitutive of the probative value of the result. A bare disclosure of outputs, unaccompanied by the methodology that generated them, does not satisfy the obligation. It is the minimum content of the Article 6 disclosure duty as applied to OSINT, and the precondition for any meaningful exercise of the adversarial right.

The second concerns the integrity of the evidentiary object. The principle of equality of arms, and the requirement that digital evidence be subject to genuine adversarial scrutiny affirmed by the Grand Chamber in *Yalçinkaya*, presuppose that the defence can examine the same material that the prosecution has relied upon. Because open-source data is liable to alteration or disappearance after the moment of collection, this requirement can be satisfied only if the material is preserved in forensically sound form at the time it is gathered, with its metadata intact and its chain of custody documented. Preservation at the point of collection is not merely a matter of good investigative practice. It is the condition on which the defence's capacity to contest the evidence depends, and its absence renders adversarial testing illusory. Where the prosecution has failed to preserve the data in such a form, it must accept the evidentiary consequences.

The third concerns independent verification. The Court's insistence in *Yalçinkaya* that domestic courts engage meaningfully with defence challenges, rather than endorse reports produced by intelligence or law-enforcement bodies, places a substantive obligation on the trial court. In the OSINT context, meaningful engagement presupposes that the court has the capacity to evaluate the technical processes by which the evidence was generated, and that the defence has the opportunity to commission its

own expert analysis of the same material. Custers (2024) has argued that the fairness of proceedings involving complex technology turns on the decision-maker's ability to evaluate the underlying processes, and the reasoning transposes directly. Where the court cannot perform that evaluation independently, and the defence cannot obtain counter-expertise, reliance on OSINT evidence takes place in conditions that Article 6 does not countenance.

None of these requirements is novel in doctrinal terms. Each follows from a line of jurisprudence already established. What is new is the insistence that they be applied consistently to OSINT evidence, and that domestic procedural law be structured to give effect to them in practice. For jurisdictions at earlier stages of development, and the Western Balkans in particular, the point at which criminal procedure codes are being reformed is also the moment at which these requirements can be embedded at the level of the statute rather than retrofitted through judicial practice. Once investigative practice becomes entrenched without corresponding procedural safeguards, the cost of subsequent correction rises considerably.

10. Conclusion

Current procedural frameworks are not equipped for OSINT evidence. The focus on expanding investigative capability, unaccompanied by corresponding procedural development, has created a structural asymmetry between prosecution and defence. The defence risks not being able to access the underlying data, examine the tools used to process it, and to be unable to replicate the conditions under which it was collected. In the Western Balkans, where these techniques are being adopted through international capacity-building programmes while criminal procedure codes remain largely unreformed in this particular area, the gap between capability and safeguard is widening.

The ECtHR has been increasingly clear on what the fair trial guarantees require when digital evidence is relied upon at trial. Zakharov, Big Brother Watch, Benedik, and most recently Yalçinkaya have established that such evidence requires a clear legal basis, safeguards operating at every stage of its collection and use, and meaningful adversarial scrutiny at trial. This article has argued that these requirements are doctrinally sufficient to govern the use of OSINT-derived evidence as well, and has identified three implications that follow from their application: disclosure of methodology, preservation in forensically sound form, and access to the underlying data in conditions that permit independent verification. The task for legislators and courts is not to invent a new framework but to give these existing requirements practical effect in a procedural environment that was not designed with OSINT in view.

The question is whether that task will be undertaken before the investigative practices to which it relates become entrenched. For the countries of the Western Balkans, currently reforming their criminal justice systems, the present circumstances provide an opportunity to legislate for fairness before practice outruns it. OSINT will inevitably become one of the primary evidentiary tools of criminal justice. If the procedural

conditions for its use do not develop alongside it, the result may be systems that satisfy Article 6 on paper while leaving the defence without real capacity to contest the evidence on which convictions rest.

References

- Aksamitowska, K. (2021). Digital evidence in domestic core international crimes prosecutions: Lessons learned from Germany, Sweden, Finland and the Netherlands. *Journal of International Criminal Justice*, 19(1), 189–211. <https://doi.org/10.1093/jicj/mqab035>
- Bărbulescu v. Romania (Grand Chamber) (2017, September 5). <https://hudoc.echr.coe.int/eng?i=001-177082>
- Bazzell, M. (2023). *OSINT techniques: Resources for uncovering online information* (10th ed.). IntelTechniques. <https://inteltechniques.com/book1.html>
- Benedik v. Slovenia (2018, April 24). <https://hudoc.echr.coe.int/eng?i=001-182455>
- Big Brother Watch and Others v. the United Kingdom (Grand Chamber) (2021, May 25). <https://hudoc.echr.coe.int/eng?i=001-210077>
- Böhm, I., & Lolagar, S. (2021). Open source intelligence: Introduction, legal, and ethical considerations. *International Cybersecurity Law Review*, 2(2), 317–337. <https://doi.org/10.1365/s43439-021-00042-7>
- Centrum för Rättvisa v. Sweden (Grand Chamber) (2021, May 25). <https://hudoc.echr.coe.int/eng?i=001-210078>
- Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/224>
- Custers, B. (2024). A fair trial in complex technology cases: Why courts and judges need a basic understanding of complex technologies. *Computer Law & Security Review*, 52, 105935. <https://doi.org/10.1016/j.clsr.2024.105935>
- Custers, B., & Stevens, L. (2021). The use of data as evidence in Dutch criminal courts. *European Journal of Crime, Criminal Law and Criminal Justice*, 29(1), 25–46. <https://doi.org/10.1163/15718174-bja10015>
- De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law* (pp. 61–104). Intersentia.
- Edwards and Lewis v. the United Kingdom (Grand Chamber) (2004, October 27). <https://hudoc.echr.coe.int/eng?i=001-67226>
- Eurojust. (n.d.). Western Balkans Criminal Justice (WBCJ) Project: Enhancing cross-border cooperation in criminal justice in the Western Balkans. Retrieved April 18, 2026, from <https://www.eurojust.europa.eu/western-balkans-criminal-justice>
- Galič, M. (2021). De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: Een suggestie voor uitbreiding. *Boom Strafbblad*, 2(2), 41–49. <https://ssrn.com/abstract=3838680>
- Ghioni, R., Taddeo, M., & Floridi, L. (2024). Open source intelligence and AI: A systematic review of the GELSI literature. *AI & Society*, 39(4), 1827–1842. <https://doi.org/10.1007/s00146-023-01628-x>
- Ladkin, P. B., Littlewood, B., Thimbleby, H., & Thomas, M. (2020). The Law Commission presumption concerning the dependability of computer evidence. *Digital Evidence and Electronic Signature Law Review*, 17, 1–14. <https://doi.org/10.14296/deeslr.v17i0.5143>
- Lagerwaard, P. (2023). Financial surveillance and the role of the Financial Intelligence Unit

- (FIU) in the Netherlands. *Journal of Money Laundering Control*, 26(7), 63–84. <https://doi.org/10.1108/JMLC-09-2022-0134>
- López Ribalda and Others v. Spain (Grand Chamber) (2019, October 17). <https://hudoc.echr.coe.int/eng?i=001-197098>
- Mason, S., & Seng, D. (Eds.). (2021). *Electronic evidence and electronic signatures* (5th ed.). Institute of Advanced Legal Studies, University of London.
- OHCHR & Human Rights Center, University of California, Berkeley. (2022). *Berkeley Protocol on digital open source investigations*. United Nations. https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf
- Quattrocchio, S., Anglano, C., Canonico, M., & Guazzone, M. (2020). Technical solutions for legal challenges: Equality of arms in criminal proceedings. *Global Jurist*, 20(1), 20190058. <https://doi.org/10.1515/gj-2019-0058>
- Roman Zakharov v. Russia (Grand Chamber) (2015, December 4). <https://hudoc.echr.coe.int/eng?i=001-159324>
- Rowe and Davis v. the United Kingdom (2000, February 16). <https://hudoc.echr.coe.int/eng?i=001-58496>
- Sachoulidou, A. (2024). Going beyond the “common suspects”: To be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*, 32(4), 1397–1445. <https://doi.org/10.1007/s10506-023-09347-w>
- Sampson, F. (2016). Following the breadcrumbs: Using open source intelligence as evidence in criminal proceedings. In B. Akhgar, P. S. Bayerl, & F. Sampson (Eds.), *Open source intelligence investigation: From strategy to implementation* (pp. 295–304). Springer. https://doi.org/10.1007/978-3-319-47671-1_18
- Sampson, F. (2017). Intelligent evidence: Using open source intelligence as evidence for serious crime. *The Police Journal: Theory, Practice and Principles*, 90(1), 55–69. <https://doi.org/10.1177/0032258X16671031>
- Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, 105575. <https://doi.org/10.1016/j.clsr.2021.105575>
- Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, 49, 105801. <https://doi.org/10.1016/j.clsr.2023.105801>
- Stoykova, R. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*, 55, 106040. <https://doi.org/10.1016/j.clsr.2024.106040>
- U.S. Department of Justice, OPDAT. (n.d.). Europe region. Retrieved April 18, 2026, from <https://www.justice.gov/criminal/criminal-opdat/worldwide-activities/central-and-eastern-europe-region>
- Wells, D., & Gibson, H. (2017). OSINT from a UK perspective: Considerations from the law enforcement and military domains. In *Proceedings of the Estonian Academy of Security Sciences*, 16, 84–113. https://shura.shu.ac.uk/17412/2/OSINT_EASS.pdf
- Yüksel Yalçinkaya v. Türkiye (Grand Chamber) (2023, September 26). <https://hudoc.echr.coe.int/eng?i=001-227636>