

The Boundaries of Privacy: Covert Intelligence Gathering, Rule of Law, and Human Rights in Comparative Perspective

Vince Vári¹, Balint Szabo²

Ludovika University of Public Service, Faculty of Law Enforcement, Budapest, Hungary

Submitted: 2026-06-19 • Accepted: 2026-07-03 • Published: 2026-08-13

Abstract: This article examines covert intelligence-gathering frameworks in six jurisdictions – Hungary, Austria, Croatia, France, the United States, and China – alongside a case study of Serbia's 2024 reform, testing a 'modernity paradox': the proposition that technological sophistication in surveillance regulation does not correlate with stronger rule-of-law protections. Using a qualitative, most-different-systems comparative design structured around three analytical domains – authorization mechanisms, technological capabilities, and human rights risk – the study develops a 'classical-adaptive-modern' typology. Particular attention is devoted to the tripartite structure of Hungarian covert intelligence law – the Nbtv. (Nemzetbiztonsági szolgálatokról szóló törvény / Act on National Security Services), Rtv. (Rendőrségről szóló törvény / Police Act), and Be. (Büntetőeljárásról szóló törvény / Code of Criminal Procedure) tracks – the historical TIGY (titkos információgyűjtés / covert intelligence gathering) / TASZ (titkos adatszerzés / covert data acquisition) dichotomy abolished by the 2017 codification, covert-detection provisions in sectoral statutes beyond the Nbtv. and Rtv., and the implications of the 2025 targeted legislative amendments. Findings confirm a structural inverse relationship: Croatia (classical) combines conservative tools with robust parliamentary oversight, while the United States and China (modern) combine extensive collection capacities with the weakest authorization regimes. Hungary, Austria, and France (adaptive) exhibit recurrent 'grey zones' where new capabilities outpace existing safeguards. Serbia's 2024 reform illustrates that typological classification represents a policy choice rather than a fixed destiny.

Keywords: covert surveillance; comparative criminal procedure; rule of law; modernity paradox; post-socialist legal systems; criminal intelligence; human rights.

INTRODUCTION

Contemporary states face the persistent challenge of balancing two competing obligations: ensuring citizen security and upholding fundamental human rights (Lazarus, 2021; Csink, 2017). Neither value is absolute; as perceived security risks increase, societies may

1 Corresponding author: vari.vince@uni-nke.hu • <https://orcid.org/0000-0001-6416-1645>

2 szabo3.balint@stud.uni-nke.hu • <https://orcid.org/0009-0006-7970-2233>



accept greater restrictions on liberty, yet neither dimension should be pursued without limitation (Csink, 2017; Zekavica, 2019). Covert intelligence gathering operates within this tension as a necessary yet inherently risky tool, justified only when legality, necessity, and proportionality are satisfied and subject to robust ex ante and ex post oversight (European Union Agency for Fundamental Rights [FRA], 2017). Technological advancements in the digital era have disrupted this balance. The proliferation of mass data collection, AI-driven analytics, and global communications has significantly enhanced the efficiency of security agencies, while simultaneously rendering privacy protections increasingly vulnerable due to legislative frameworks lagging behind technological innovation.

This article contends that technological advancement in covert-intelligence regulation does not inherently correspond to a higher standard of rule-of-law protections. Instead, a paradox emerges: states utilizing the most advanced surveillance tools often rely on broadly defined legal frameworks, which pose heightened risks to human rights (Richards, 2013). Recent scholarship supports this observation, indicating that surveillance-oriented governance models frequently outpace the development of privacy-preserving legal regimes (Saputra & Handayani, 2024). Furthermore, the commercial logic underlying surveillance capitalism produces structural parallels to state surveillance by normalizing large-scale behavioral data extraction without meaningful consent (Zuboff, 2019). In contrast, technologically conservative states typically emphasize legal certainty through detailed, guarantee-oriented legislation (FRA, 2017; Geneva Centre for Security Sector Governance, 2015). For the purposes of this study, 'covert intelligence gathering' denotes the lawful acquisition of information by state authorities through means concealed from the affected person – interception of communications, covert surveillance, access to computer systems, and human sources – for national-security or criminal-procedure purposes (FRA, 2017; Born & Wills, 2013). This definition encompasses both national-security and criminal-procedure tracks, since the same technique may be regulated under either heading depending on the purpose invoked – a dualism treated throughout as a central object of comparison (Ilijevski & Krstevska-Savovska, 2021; Živanović, 2018). In the Hungarian doctrinal literature, 'covert detection' (titkos felderítés) functions as an umbrella concept that divides into covert measures applicable within criminal proceedings (leplezett eszközök) and intelligence gathering authorized under sectoral statutes (titkos információgyűjtés); five distinct operational objectives are distinguishable – law enforcement, national security, policing, counter-terrorism, and internal protection – each requiring different institutional frameworks and different guarantees (Csizner, 2024; Finszter, 2024).

The jurisdictions selected for analysis are not randomly chosen within the broader field of surveillance scholarship. Hungary, Croatia, and Serbia represent post-socialist states whose covert-intelligence frameworks underwent significant restructuring following 1989–1990, marking a legal transition that remains relatively underexplored in comparative research (Connell, 2007; Carrington et al., 2016).

THEORETICAL FRAMEWORK

The analysis is grounded in two theoretical frameworks. Securitization theory elucidates the framing of covert intelligence gathering as a 'necessary but perilous instrument,' whereby issues are elevated from ordinary politics and depicted as existential threats,



thereby justifying otherwise unacceptable measures (Buzan et al., 1998). Additionally, the 'classical-adaptive-modern' typology serves as a set of Weberian ideal types – abstract, intentionally simplified constructs used to evaluate concrete systems (Weber, 1949).

The doctrinal foundation for assessing covert intelligence under the European Convention on Human Rights (ECHR) developed cumulatively. *Klass v. Germany* (1978) established that covert surveillance may interfere with Article 8 but can be justified if 'necessary in a democratic society' and grounded in clear, accessible law. *Huvig v. France* (1990) added the 'quality of law' requirement. *Roman Zakharov v. Russia* (2015) consolidated minimum safeguards: the nature of offenses, categories of persons, duration limits, and procedures for authorization, examination, use, storage, and erasure. Szabó and Vissy v. Hungary (2016) found Hungary's national-security surveillance regime in violation of Articles 8 and 13, owing to the absence of a reasonable-suspicion threshold, the breadth of ministerial authorization, and the lack of effective ex post remedies – deficiencies whose implications for evidentiary admissibility are analyzed in the literature of *NBP. Nauka, bezbednost, policija* – NBP (Živanović, 2018). *Big Brother Watch v. United Kingdom* (2021) extended this logic to bulk interception, requiring 'end-to-end safeguards'. The State's positive obligation under Article 2 further informs this framework, since inadequate oversight may expose individuals to lethal threats without legal redress (Šurlan, 2021).

RESEARCH QUESTIONS AND HYPOTHESES

The research addresses three primary questions: (RQ1) whether a structural, inverse relationship exists between technological sophistication and rule-of-law safeguards (the 'modernity paradox'); (RQ2) whether national frameworks can be systematically categorized into ideal types with explanatory utility; and (RQ3) whether a state's typological classification is static or subject to change through deliberate policy interventions. Correspondingly, three hypotheses are proposed: H1 (modernity paradox) posits that technologically advanced states will demonstrate weaker oversight and greater human-rights risks; H2 (adaptive grey-zone hypothesis) anticipates that adaptive states will exhibit regulatory grey zones where new capabilities surpass existing authorization frameworks; and H3 (dynamism hypothesis) suggests that typological classification can shift within a single legislative reform cycle.

METHODS

This study utilizes a qualitative, comparative legal methodology, interpreting national regulations as manifestations of underlying policy choices and institutional logics (Oderkerk, 2025). Six diverse jurisdictions – Hungary, Austria, Croatia, France, the United States, and China – are selected using a most-different-systems approach, maximizing variation in legal family, regime type, and geopolitical context while maintaining the presence of a legal framework for covert intelligence gathering (Przeworski & Teune, 1970; Ankar, 2008). These cases were deliberately chosen to reflect not only geographical diversity but also distinct traditions of legal regulation, models of intelligence governance, and stages of democratic development, from post-socialist transitions (Hungary, Croatia, Serbia), to



consolidated democracies (Austria, France, United States), and an authoritarian context (China). The selection enables a robust comparative test of the ‘modernity paradox’ across divergent systems. However, while the range enhances theoretical generalizability, the findings remain most relevant to jurisdictions with established covert surveillance frameworks and may not capture dynamics present in states lacking such legal instruments. Each jurisdiction is analyzed across three domains: authorization mechanisms, technological capabilities, and human rights risk (FRA, 2017). Special emphasis is placed on the policeware dimension; as Pisarić (2023) notes, state-sponsored malware-based hacking represents a distinct covert tool category necessitating explicit statutory regulation rather than mere extension of existing interception provisions. Serbia’s 2024 reform is included as a theory-testing case study to address RQ3/H3.

RESULTS

HUNGARY

Hungary’s covert-intelligence framework is, among the six jurisdictions examined, structurally the most complex: it rests on three procedurally distinct tracks, each governed by its own statute and each operating with its own authorization chain, while remaining connected through carefully constructed boundary rules and cross-track evidence provisions. Figure 1 provides a structural overview.

The Three-Track Architecture

The immediate post-transition settlement was established by Act X of 1990, which transitionally regulated special intelligence tools before the more durable 1995 framework (Nbtv., Act CXXV of 1995) replaced it (Jancsó, 2018). The three tracks that emerged – and that the 2017 codification preserved while reconfiguring the third—are analytically distinct but procedurally connected.

Track I (Nbtv.-track) encompasses titkos információgyűjtés by national security services for national security purposes. Under Nbtv. §13, the most intrusive methods – secret searches, interception of communications, and access to computer systems – require the authorization of the Minister of Justice, a political appointee. In urgent cases, the service’s Director-General may grant interim authorization pending subsequent ministerial approval. The critical structural feature of this track is that it contains no mandatory, independent judicial pre-authorization, and that the right to post-surveillance notification – formally preserved by Nbtv. §13(5) – is subject to discretion, providing no guaranteed remedy to the affected person (Csizner, 2021; FRA, 2022b).

Track II (Rtv.-track) governs the general police’s titkos információgyűjtés for crime-prevention purposes under the Police Act (Rtv., Act XXXIV of 1994). Rtv. §63(4) establishes that the police may deploy leplezett eszközök for offense-related purposes exclusively under the Code of Criminal Procedure; the Rtv.’s own track is confined to the pre-procedural crime-prevention objectives of §64. For the most intrusive tools (§§70–75/E), judicial authorization is required; for less intrusive methods (§66), an internal order suffices. Empirical data for the first half of 2020 recorded 1,285 applications of covert-intelligence tools



in the crime-prevention policing track, of which 561 occurred in the preparatory phase of investigations (Győri & Szendrei, 2021).

TRACK I Nbtv.-track (Act CXXV/1995)	TRACK II Rtv.-track (Act XXXIV/1994)	TRACK III Be.-track (Act XC/2017)
National-security intelligence gathering (titkos információgyűjtés)	Crime-prevention covert gathering (titkos információgyűjtés)	Criminal-procedure covert measures (leplezett eszközök)
AUTHORISATION Minister of Justice No mandatory prior judicial authorisation Urgent cases: Director-General + subsequent ministerial approval	AUTHORISATION Judicial authorisation for most intrusive tools (Rtv. §§70–75/E) Internal order for less intrusive tools (§66)	AUTHORISATION Tiered authorisation: • Internal order • Prosecutorial order • Pre-trial judge order (taxative list — Be. §244)
Key tools Communication interception Secret search · Remote IT access HUMINT operations	Key tools Targeted interception Location data · Physical surveillance HUMINT (pre-procedural)	Key tools Interception · Covert search IT system monitoring Undercover officer
Main actors AH · IH · KNBSZ (+TEK under Nbtv.)	Main actors Police (general) (+TEK under Rtv.)	Main actors All feljogosított hatóságok (TEK · NAV · Military)
titkos információgyűjtés	titkos információgyűjtés	leplezett eszközök
TERRORELHÁRÍTÁSI KÖZPONT (TEK) — Counter-Terrorism Centre		

Note: AH = Alkotmányvédelmi Hivatal (Office for the Protection of the Constitution); IH = Információs Hivatal (Information Office); KNBSZ = Katonai Nemzetbiztonsági Szolgálat (Military National Security Service); NAV = Nemzeti Adó- és Vámhivatal (National Tax and Customs Administration); IRM = igazságügyi miniszter (Minister of Justice). IMSI-catchers are not yet formally authorized in Hungary (cf. the 2024 reform in Serbia, discussed in the text).

Figure 1. *The Three-Track Structure of Hungarian Covert Intelligence Law*

Track III (Be.-track) governs leplezett eszközök within criminal proceedings under the Code of Criminal Procedure (Be., Act XC of 2017). Be. §214(2) establishes that authorized investigative authorities may deploy leplezett eszközök exclusively under the Be.; Be. §214(3) expressly preserves, however, that this criminal-procedure exclusivity does not affect the titkos információgyűjtés of national security services and the Counter-Terrorism Center (TEK) under the Nbtv. track. The Be. introduces a tiered authorization framework: tools requiring internal order, tools requiring prosecutorial order, and tools requiring a pre-trial judge's order (exhaustive list: Be. §244). The result is a substantially stronger guarantee architecture than the Nbtv. track, with broader judicial oversight, stronger proportionality requirements, and clearer exclusionary rules.

Cross-track evidence transfer is governed by Be. §§259–260: Nbtv.-track material is admissible in criminal proceedings provided that the conditions governing its acquisition were satisfied and that it is used to prove an offense for which a judicially authorized leplezett eszközök could have been deployed (Bárándy & Enyedi, 2018). This creates a normatively significant asymmetry: the more rigorous Be.-track controls can, in effect, be bypassed if the gathering authority originally invokes the Nbtv. track.



The Abolition of the TIGY/TASZ Dichotomy

Pre-2018 Hungarian law applied two sharply distinct terminological systems for covert measures in the criminal justice context. Titkos információgyűjtés (TIGY, literally ‘covert information gathering’) – regulated under the Rtv. and sectoral statutes – was applicable before proceedings were initiated, for the purpose of detecting or preventing an offense, and without a suspicion requirement. Titkos adatszerzés (TASZ, literally ‘covert data acquisition’) – regulated under the 1998 Code of Criminal Procedure (Act XIX/1998) – was available only within ongoing criminal proceedings and required reasonable suspicion (alapos gyanú) as an activation threshold, i.e. a substantiated factual basis for believing a specific person had committed a specific offence (Bárándy & Enyedi, 2018).

The 2017 Be.’s most significant structural innovation was the abolition of this dichotomy: the unified category of leplezett eszközök subsumed both the criminal-procedure dimension of TIGY and TASZ under a single framework, simultaneously creating a more coherent authorization regime and more consistent exclusionary rules for the Be.-track (Jancsó, 2018). This reform was directly motivated by the ECHR’s 2016 findings: the legislative response to Szabó and Vissy consisted of strengthening the purposive linkage of covert tools, making judicial pre-authorization mandatory for the most intrusive measures, and expanding prosecutorial supervision within the Be.-track (Jancsó, 2018). The terminological unification, however, was confined to the Be.-track. The Nbtv. and Rtv. tracks continue to operate under the titkos információgyűjtés designation with their own, pre-existing terminological and procedural frameworks.

Sectoral Laws: A Polyarchic, Not Bipolar, Structure

An account restricted to the Nbtv./Rtv./Be. Triad risks understating the true breadth of Hungarian covert-detection law. Multiple sectoral statutes create their own covert-intelligence powers calibrated to their respective institutional mandates (Nyeste, 2012; Nyeste & Szendrei, 2019). The National Tax and Customs Authority Act (NAV Act, Act CXXII/2010) grants the NAV’s investigative and detection units covert-gathering powers for tax and customs offenses, with judicial authorization required for the most intrusive tools and internal orders sufficient for less intrusive methods. The Defense Act (Act CXIII/2011) provides military intelligence and counterintelligence services with their own frameworks, which partly diverge from the Nbtv. architecture. The Prosecution Service Act (Ütv., Act CLXIII/2011) gives the prosecution’s investigative authority the statutory basis to deploy Be.-track leplezett eszközök, with mandatory prosecutorial supervision. The result is a polyarchic rather than bipolar structure: the authorization thresholds – particularly the judicial-authorization threshold – differ across organs performing comparable functions, creating disproportionate inequality of protection for individuals who happen to be targeted by different authorities (Nyeste, 2018).

Internal Contradictions in the Be.-Track Judicial Authorization Regime

Within the Be.-track, the exhaustive list of judicially authorized tools (Be. §244) reveals an internal inconsistency between the invasiveness of a given tool and the intensity of its authorization requirement: certain objectively more intrusive methods are subject to lower authorization standards, while some less intrusive tools fall within the judicial-authorization category (Steiner, 2023). The covert monitoring of IT systems, which enables access



to the entirety of a subject's digital activity and is objectively more invasive than traditional telecommunications interception, is not invariably subject to a mandatory proportionality assessment in the authorization procedure examining the volume of data made accessible (Steiner, 2023). This gap connects directly to the 'end-to-end safeguards' requirement articulated in Big Brother Watch: the judicial order must specify not merely the person but the categories of communications and the selectors, a requirement the current Be. framework does not consistently operationalize for IT system monitoring. The practical consequences of these inconsistencies are illustrated when, for instance, law enforcement authorities obtain authorization to covertly monitor a suspect's entire IT system under a lower threshold than would be required for telephone tapping, thereby gaining access to large volumes of personal data without a detailed judicial assessment of necessity and proportionality. In a hypothetical case, evidence obtained from such broadly authorized IT system monitoring might later be challenged in court on the grounds that the order did not specify selectors or categories of data, resulting in the exclusion of key evidence and the collapse of the prosecution's case, even where serious criminal conduct is involved. Conversely, investigators using less intrusive techniques may be required to undergo a more stringent judicial process, creating disincentives to targeted surveillance and incentivizing the use of broader, less regulated methods. Additionally, the practical admissibility constraints of covert-tool evidence operate bidirectionally: if the authorization procedure's formal requirements are not observed, the obtained data cannot be valorized as evidence at trial, risking compromise of the prosecution's case – a tension documented in the prosecutorial literature (Farkas, 2022; Steiner, 2021).

The TEK's Cross-Track Position and Organizational Asymmetry

The TEK, established under Act CXLVII/2010, occupies a position within the Hungarian three-track system without parallel in any of the other five jurisdictions: it operates simultaneously under all three tracks. In its policing capacity, the TEK falls under the Rtv. In its national-security capacity, the TEK operates under the Nbtv. – and Be. §214(3) expressly preserves this power despite the Be.'s exclusivity principle. In its law-enforcement capacity, the TEK constitutes a *feljogosított szerv* (authorized authority) under the Be., capable of deploying *leplezett eszközök* in criminal proceedings. This trifold empowerment means that the TEK is the only actor in the system for which the cross-track evidence provisions of Be. §§259–260 regularly apply to its own earlier-gathered material.

This contrasts sharply with the position of the civilian intelligence services – the Alkotmányvédelmi Hivatal (AH, Office for the Protection of the Constitution) and the Információs Hivatal (IH, Information Office). These services operate exclusively under the Nbtv. track: they are not enumerated as *feljogosított szervek* under the Be. and are excluded from the Rtv.'s scope. The AH cannot, therefore, directly deploy a Be.-track *leplezett eszköz* even where its intelligence-gathering reveals an imminent criminal offense; it must transfer the material to a competent investigative authority or to the TEK. The normative consequence is that the guarantee of the Nbtv. track – particularly the absence of mandatory judicial pre-authorization and the restricted post-surveillance notification – affects not only the most powerful cross-track actor (TEK) but also the civilian services for whose activities no alternative judicial avenue exists (Csizner, 2024).



The 2025 Amendments

Acts CXXVII and CXXVIII of 2025 amended, respectively, the Nbtv's national-security vetting procedures and certain sectoral statutes ancillary to the *leplezett eszközök* framework. Neither Act amended the Be. nor the Rtv. themselves; both are thus targeted corrections rather than structural recodification. Crucially, the Nbtv's ministerial-authorization chain – and the structural guarantee deficit identified by Szabó and Vissy and maintained since by the Committee of Ministers' supervision – remained unchanged by both Acts.

The Pegasus Affair and the Article 13 Deficit

The practical stakes of the guarantee architecture were demonstrated by the 2021 Pegasus affair. A forensic investigation established that over 300 Hungarian nationals – including journalists, lawyers, and figures associated with the opposition – appeared on an NSO Group targeting list (Amnesty International, 2021). The government acknowledged that it had procured Pegasus for national security surveillance within the existing Nbtv. framework (European Parliament, 2023); no substantive public disclosure was made about targeting decisions or the authorization process. The National Authority for Data Protection and Freedom of Information (NAIH) (2022) investigation closed without actionable results – its findings classified until 2050 – precisely replicating the structural deficiency Szabó and Vissy identified as an Article 13 violation: a formally existing supervisory body capable of exercising no meaningful supervision (Csizner, 2021). The episode illustrates the proportionality and oversight gap that arises when authorities deploy policeware – technically sophisticated malware for remote device access (Pisarić, 2023) – under a broadly defined, ministerially authorized national-security provision without the end-to-end safeguards required by Big Brother Watch and extended to signals-intelligence bulk collection by *Centrum för rättvisa v. Sweden* (2021).

AUSTRIA

Following the 2018 BVT affair (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* – BVT), in which an anti-corruption police raid on the domestic intelligence service's own headquarters resulted in the seizure of sensitive files, lasting damage to Austria's position in international intelligence-sharing arrangements such as the Club de Berne, and the documented failure to act on prior warnings ahead of the 2020 Vienna terrorist attack – Austria replaced the BVT with the Directorate for State Protection and Intelligence (DSN) under the State Protection and Intelligence Service Act (SNG, BGBl. I Nr. 5/2021) (Fux et al., 2023). The SNG establishes a two-tiered authorization process: initial approval by an independent Legal Protection Commissioner (*Rechtsschutzbeauftragter*) and review by a dedicated Federal Administrative Court senate. The Commissioner's appointment by the federal government raises persistent questions about functional independence (Fux et al., 2023). A 2025 draft law would extend this chain to DSN monitoring of encrypted messenger communications of identified threat individuals, framing the extension as an ultima ratio measure – illustrating how Austria's adaptive classification results from incrementally extending an only partially independent authorization architecture to newly capable tools, a pattern that oversight literature identifies as the defining structural vulnerability of reformed security systems (Ilijevski & Krstevska-Savovska, 2021). The doctrinal roots



lie in the Austrian Constitutional Court's G 72/2019 ruling, which struck down the predecessor framework's Bundestrojaner provisions as incompatible with the right to privacy for lacking procedural safeguards or necessity thresholds – concerns directly analogous to Huvig's quality-of-law principle.

CROATIA

Croatia's framework consciously prioritizes accountability as a legacy of its break from the Yugoslav security apparatus (UDBA). The Security and Intelligence System Act establishes multiple supervisory layers, most notably a national security committee chaired by a member of the largest opposition party, providing substantive rather than merely formal parliamentary oversight (Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, 2006; FRA, 2017). Croatia's toolkit remains traditional and targeted, offering the most robust procedural guarantees among the six jurisdictions. One internal tension exists: the Criminal Procedure Code permits unlawfully obtained evidence in serious crime proceedings where the public interest in prosecution outweighs the infringement of rights (Krapac, 2010) – a proportionality logic that also underpins the limited rule-breaking privileges extended to undercover operators (fedett nyomozók) who infiltrate criminal organizations.

FRANCE

France combines high centralization in national security matters with specialized judicial control in criminal investigations. The Internal Security Code authorizes the Prime Minister to approve covert intelligence gathering, with the National Oversight Commission for Intelligence-Gathering Techniques (Commission Nationale de Contrôle des Techniques de Renseignement – CNCTR) as oversight authority (Code de la sécurité intérieure, 2012; Commission Nationale de Contrôle des Techniques de Renseignement, 2024). For criminal investigations, the judge of liberties and detention (juge des libertés et de la détention – JLD) controls the most intrusive measures, exercising genuine structural independence from the trial judiciary (FRA, 2022a). France and Hungary both operate multi-track architectures; France's 'police administrative' track, however, subsumes both national security and organized crime prevention, without a distinct intermediate crime-prevention track, leaving it a two-track rather than a three-track system. For the 2024 Olympic Games, Article 10 of Law No. 2023-380 authorized experimental AI-driven 'augmented cameras' with sunset provisions and mandatory ex post evaluation, subject to the National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés – CNIL) continuous compliance supervision – a markedly more regulated introduction of a new capability than Hungary's Pegasus deployment (Loi n° 2023-380, 2023).

UNITED STATES

The United States exemplifies an efficiency-driven model in which national-security imperatives frequently subordinate privacy. The 2024 Reforming Intelligence and Securing America Act (RISAA) reauthorized Section 702 of the Foreign Intelligence Surveillance Act (FISA) while broadening provider obligations and extending the scope of 'foreign in-



telligence information' to international narcotics offenses, leaving the Foreign Intelligence Surveillance Court (FISC) classified *ex parte procedure intact* (Liu, 2024). As Richards (2013) argues, the chilling effect generated by such architectures on lawful expressive and associational activity constitutes a harm independent of any specific surveillance act – one that the U.S. framework's design systematically fails to address. A 2025 federal district court ruling held that 'backdoor searches' of Section 702-collected data using identifiers of U.S. persons ordinarily require a warrant; as of this writing, no statutory change has followed. Each successive legislative cycle has expanded the scope of mass collection while leaving the core oversight deficit unresolved.

CHINA

China's framework follows a fundamentally different logic: not to limit state power but to enable the Party's objective of total intelligence control, an arrangement in which legal instruments remain subordinate to Party leadership (Horsley, 2019). The National Intelligence Law (National People's Congress, 2017) requires every organization and citizen to support, assist, and cooperate with state intelligence work (Article 7), while China's Personal Information Protection Law (National People's Congress, 2021) explicitly exempts national-security and public-security processing from its general requirements – formalizing the carve-out this article identifies as definitional of the 'modern' category. Unlike the case-specific authorization tests that structure the other five jurisdictions, Article 7 establishes a generalized, citizenship-wide cooperation obligation that logically precedes any individualized authorization. The surveillance architecture Haggerty and Ericson (2000) describe as a 'surveillant assemblage' operates in China through state-directed rather than commercially dispersed networks, achieving a degree of comprehensive behavioral monitoring without parallel in any of the other five jurisdictions (Human Rights Watch, 2019).

SERBIA: 2024 REFORM

Serbia's pre-2024 framework firmly occupied the classical position: traditional investigative methods, judicially authorized telecommunications interception, and no legal basis for IMSI-catchers or intrusive software. The 2024 reform of the Code of Criminal Procedure responded simultaneously to EU accession pressure (European Commission, 2024) and internal investigative demands from prosecutors facing encrypted communications and transnational criminal networks. It introduced IMSI-catchers as a formally recognized covert tool, anchored in a specific written warrant issued by a pre-trial judge, confined to a closed list of the gravest offenses, and subject to an explicit subsidiarity requirement ("Serbia's Unregulated Use", 2024; European Digital Rights [EDRi], 2024). By binding a new technological capability to a reinforced – rather than merely extended – authorization regime contemporaneously, Serbia's transition from classical to adaptive demonstrates that the modernity paradox is not an absolute law but a conscious policy choice.

Despite this formal classical profile, documented surveillance abuses undermined confidence in the Serbian framework. Amnesty International's 2024 'Digital Prison' investigation documented the deployment of Pegasus spyware and a custom Android surveillance tool called NoviSpy against Serbian journalists, activists, and civil society representatives,



as well as covert use of IMSI-catchers by the police without any statutory basis (Amnesty International, 2024). The report established a pattern in which technically sophisticated tools were deployed outside the special investigative measures' framework – precisely the same structural dynamic that characterises the adaptive grey zones identified in Hungary, Austria, and France. Reform proposals advanced in the Serbian security-sector literature had already identified this gap between formal regulation and operational practice (Milosavljević, 2023). Prior to the 2024 reform, Serbia therefore exhibited a bifurcated character: a formally classical legal framework coexisting with documented classical/adaptive-boundary violations in operational practice.

The 2024 reform of the Code of Criminal Procedure responded to two simultaneous pressures. First, Chapter 23 (fundamental rights) of Serbia's EU accession process increasingly required demonstrable alignment of surveillance regulation with ECHR standards; the European Commission's 2024 Serbia Report explicitly identified the regulation of special investigative measures as a key benchmark (European Commission, 2024). Second, the Amnesty International documentation had made the absence of a legal basis for IMSI-catchers publicly untenable. The reform introduced IMSI-catchers as a formally recognised special investigative measure, embedded in a reinforced authorization structure: a specific, written, reasoned warrant issued by a pre-trial judge upon the public prosecutor's application; confinement to a closed statutory list of the gravest offences; an explicit subsidiarity requirement that the investigative aim cannot reasonably be achieved through less intrusive means; and strict time limits analogous to those governing other special investigative measures ("Serbia's Unregulated Use", 2024; EDRI, 2024). These changes respond directly to the divergences between the Serbian Code of Criminal Procedure and ECtHR standards documented in the comparative literature (Turanjanin, 2022).

The normative significance of Serbia's 2024 reform lies not in the technology adopted – IMSI-catchers are technically less sophisticated than the Pegasus spyware that Hungary deployed under the Nbtv. umbrella – but in the architecture of introduction. Hungary incorporated Pegasus into a pre-existing, broadly defined national-security track without any contemporaneous statutory adaptation, generating a grey zone that remains unresolved. Serbia introduced a new capability simultaneously with a purpose-built, reinforced legal basis. This 'contemporaneous recalibration' model, as opposed to the 'retrospective extension' pattern observed in adaptive states, provides the clearest empirical illustration of H3: typological classification is not determined by the technology adopted, but by the legislative architecture chosen to govern it. The reform also illustrates that the modernity paradox is not inevitable: a state can simultaneously upgrade its technological capacity and maintain or strengthen its authorization standards, if the political will and institutional capacity to do so exist.

DISCUSSION

AUTHORIZATION MECHANISMS

Authorization mechanisms span a spectrum from executive-centric to judicial- or guarantee-focused models. Hungary's national-security framework vests final authority in the



Minister of Justice; China represents the absolute form where independent authorization is effectively non-existent; Croatia and post-2024 Serbia exemplify the judicial pole. The United States represents the most complex hybrid: the FISC provides a veneer of judicial oversight, but its secrecy and the breadth of Section 702 render the system functionally closer to executive-centric models (Council of Europe, European Commission for Democracy through Law, 2015; FRA, 2017, 2023; Greene & Rodriguez, 2014). A critical cross-cutting dimension concerns the porousness of inter-track boundaries. Hungary and Austria both operate three-track architectures – the Nbtv./Rtv./Be. triad and the SNG/SPG/StPO triad, respectively – each with explicit boundary rules: Be. §214(3) preserves the Nbtv. track despite Be. Exclusivity. The Austrian SPG § 21(2) provides that once a person becomes a suspect, only the StPO applies. The risk that authorities shift cases to the national-security track to obtain more permissive ministerial authorization represents a structural vulnerability documented in both the comparative oversight literature and NBP scholarship (Živanović, 2018; Ilijevski & Krstevska-Savovska, 2021).

TECHNOLOGICAL CAPABILITIES AND POLICEWARE

The modern group – the United States and China – is distinguished by its mass data-collection capacity. The adaptive group – Hungary, Austria, France – has integrated modern tools (Pegasus, government-Trojan software, AI-assisted analytics) on a scale short of the modern group. Critically, the deployment of policeware within the adaptive group has consistently preceded statutory regulation: as Pisarić (2023) demonstrates through comparative analysis of Germany and the Netherlands, only explicit, purpose-specific legislative provisions with robust procedural safeguards – including prior judicial approval, subsidiarity requirements, mandatory ex post notification, and reporting obligations – can adequately govern malware-based investigation. The internal Be.-track inconsistencies between invasiveness and authorization level identified by Steiner (2023) compound this problem: where proportionality assessment is not mandatory for IT system monitoring, the gap between what the tool can access and what the authorization procedure actually examines is structurally analogous to the grey zones generated by policeware deployment without a specific legal basis. Comparative work on European data-retention regimes documents the same divergence between formal legal bases and actual collection practice (Birrer et al., 2023). The classical group – Croatia – remains most conservative, without a legal basis for mass collection or policeware.

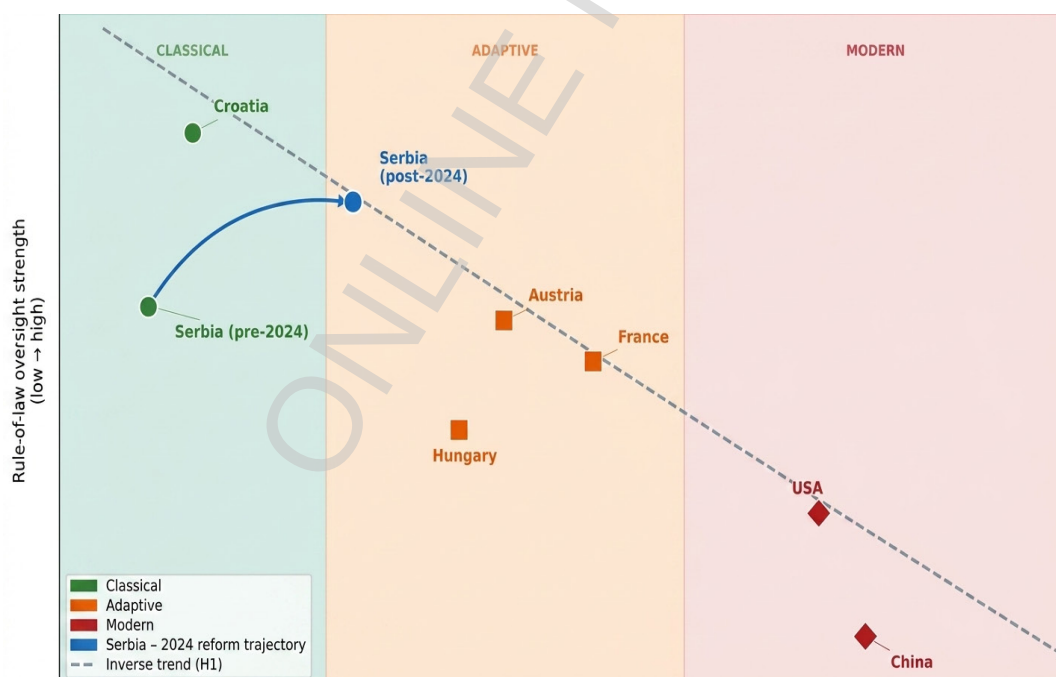
Human rights risk reveals the modernity paradox most starkly: as technological capacity increases, the specificity of legal protection tends to decrease. However, the ways in which these risks manifest differ considerably across jurisdictions. In the United States, the centralization of foreign intelligence collection under Section 702 has resulted in large-scale data access with minimal individualized judicial oversight, and the classified nature of the FISC further restricts redress for affected individuals. China's regime presents the clearest example of systematic human rights risk, where the National Intelligence Law imposes generalized surveillance obligations and the exemption of national security processing from privacy legislation enables widespread, unchecked monitoring of citizens (Human Rights Watch, 2019). In adaptive systems like Austria and France, risks often emerge in legal ambiguities as new technologies are incorporated before adequate safeguards are



legislated and as oversight bodies struggle to keep pace with the operational expansion of security services. France's AI-driven surveillance during the 2024 Olympics, for example, prompted significant public debate about the effectiveness of oversight despite sunset clauses and ex post reviews; the technical literature argues that privacy-by-design architectures can reconcile automated video analysis with data-protection requirements, which relocates the decisive question from technical capability to regulatory design (Cucchiara et al., 2024). Croatia, in contrast, mitigates risk through strict parliamentary supervision and strict exclusionary rules, although proportionality exceptions for grave crimes reflect a potential vulnerability in the system's practical operation. Hungary's Pegasus controversy exemplifies the adaptive grey zone, with a powerful tool legally justified under a broadly defined, executive-controlled national-security provision that bypasses more rigorous criminal-procedure oversight – a dynamic privacy scholarship identifies as corrosive to individual autonomy (Richards, 2013; Solove, 2011). The practical consequence in Hungary is that the admissibility constraints documented by Farkas (2022) and Steiner (2021) in the Be.-track serve as only a partial corrective: they apply to Be.-track evidence, not to the Nbtv.-track material whose classification may remain opaque until 2050.

CLASSIFICATION AND HYPOTHESIS ASSESSMENT

Figure 2 provides a qualitative positional representation of all seven cases on the two key dimensions. Table 1 presents the final typological classification.



Note: Positions are qualitative approximations grounded in the three-domain analysis. The dashed line illustrates the inverse trend constituting the modernity paradox (H1). Serbia's arrow indicates the trajectory of the 2024 reform (H3).

Figure 2. *The Modernity Paradox: Inverse Relationship Between Technological Capability and Rule-of-Law Oversight Strength Across Six Jurisdictions, with Serbia's 2024 Reform Trajectory*

Table 1. *Classification of Six Jurisdictions Within the 'Classical-Adaptive-Modern' Typology, with Serbia's Post-2024 Reform Trajectory*

Country	Technological model	Authorization model	Primary HR risks	Classification
Croatia	Traditional / HUMINT	Parliamentary / Judicial	Procedural inconsistency	Classical
Austria	Integrated digital	Independent Commissioner / Judicial	Oversight independence gaps	Adaptive
Hungary	Integrated digital	Dualistic (ministerial + judicial)	Regulatory grey zones; Pegasus affair	Adaptive
France	Integrated AI-assisted	Hybrid executive-judicial	Centralisation of power	Adaptive
USA	Mass surveillance	Hybrid (FISC)	Weak substantive authorization	Modern
China	Mass social control	Non-existent (Party control)	Arbitrary power; no redress	Modern
Serbia (post-2024)	Traditional → IMSI-catcher	Pre-trial judicial warrant (new)	Residual oversight capacity gaps	Classical → Adaptive

Note: The classification reflects the final synthesis across all three analytical domains. Serbia is shown post-2024 reform.

With respect to H1, evidence consistently supports the modernity paradox: no jurisdiction combines a 'modern' technological profile with a 'classical' authorization regime, or vice versa. H2 is confirmed by the adaptive category: Hungary, Austria, and France each independently generated public controversies of the same structural kind, despite belonging to different legal families with different baseline authorization architectures – suggesting that the grey zone is a structural feature of the adaptive position rather than an artifact of any one jurisdiction's design. H3 is confirmed by Serbia, whose 2024 reform altered typological classification within a single legislative cycle by accompanying a new capability with a contemporaneous recalibration of the governing authorization regime – demonstrating that whether a transition is smooth or contested depends less on the technology adopted than on this contemporaneous recalibration.

CONCLUSIONS

This comparative analysis empirically corroborates the modernity paradox: technological sophistication does not correspond to enhanced rights protections. Classical regimes (Croatia) confer superior legal certainty notwithstanding technological conservatism; adaptive regimes (Hungary, Austria, France) navigate persistent tension between innovation and rule-of-law obligations, generating recurrent grey zones; modern regimes (United States,



China) prioritize operational efficacy over privacy. Serbia's 2024 reform exemplifies the non-static character of these classifications, underscoring the need for perpetual renegotiation between securitization and liberty as technology advances (Born & Wills, 2013).

For Hungary specifically, the comparative analysis grounds four normative proposals. First, the Nbtv.-track's ministerial-authorization mechanism – which the European Court of Human Rights (ECtHR) identified in Szabó and Vissy as an Article 8 and 13 violation and which remains unmodified by the 2025 amendments – must be replaced or supplemented by genuinely independent, judicial or quasi-judicial prior control, in line with the consolidated requirements of Roman Zakharov and Centrum för rättvisa; the Austrian Rechtsschutzbeauftragter/Administrative Court senate model is a relevant reference, subject to the necessary correction that the Commissioner's appointment procedure must secure real independence from the executive. Second, the Be.-track judicial authorization for covert IT system monitoring must include a mandatory proportionality assessment encompassing the volume and categories of data made accessible, aligning Hungarian practice with the selector-specific authorization standard articulated in Big Brother Watch and operationalized by Pisarić (2023) in a comparative analysis of Germany and the Netherlands. Third, where new technological capacities – such as IMSI-catchers – are introduced into the Hungarian framework, the Serbian model's approach of contemporaneous, rather than retrospective, safeguard construction should be adopted: a specific written pre-trial judicial warrant, a closed offense list, and a statutory subsidiarity requirement from the outset. Fourth, the polyarchic sectoral-law structure – Nbtv., Rtv., NAV Act, Ütv., defense legislation – generates disproportionate inequality of protection for individuals targeted by different authorities applying divergent judicial-authorization thresholds for comparable tools; horizontal harmonization of guarantee standards across these instruments is required (Nyeste & Szendrei, 2019).

Two normative observations transcend the Hungarian context. First, autonomous oversight bodies staffed by multidisciplinary specialists in law, technology, and operational practice are needed in all adaptive jurisdictions to adjudicate grey zones (Born & Leigh, 2005), particularly where new capabilities cross inter-track boundaries. To maximize their effectiveness, such bodies should be constituted through transparent, merit-based appointment procedures that require broad political consensus, such as supermajority approval by parliament. Mandates should require periodic public reporting with non-classified summaries, include clear independence guarantees (such as fixed terms and removal only for cause), and require continuous training in emerging surveillance technologies. Additionally, these bodies should be empowered to access all relevant data and to trigger independent audits when new intelligence methods are introduced. Second, in response to Juvenal's perennial question, *Quis custodiet ipsos custodes?* ('Who watches the watchmen?'), effective guardianship ultimately depends on sustained societal engagement with privacy as a structural precondition for autonomous self-governance (Solove, 2011; Lyon, 2004, 2019). Two limitations follow: reliance on open-source instruments precludes assessment of classified operational practice, and rapid technological evolution renders any cross-sectional classification provisional.

Acknowledgements: The authors declare no conflict of interest. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.



REFERENCES

- Amnesty International. (2021). *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*. <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/>
- Amnesty International. (2024). *Serbia: A digital prison – Surveillance and the suppression of civil society*. <https://www.amnesty.org/en/documents/eur70/8814/2024/en/>
- Anckar, C. (2008). On the applicability of the most similar systems design and the most different systems design in comparative research. *International Journal of Social Research Methodology*, 11(5), 389–401. <https://doi.org/10.1080/13645570701401552>
- Bárándy, G., & Enyedi, K. (2018). Leplezett eszközök és titkos információgyűjtés, avagy az új büntetőeljárási törvény margójára [Covert measures and secret intelligence gathering: marginal notes on the new Code of Criminal Procedure]. *Belügyi Szemle*, 66(1), 97–104.
- Birrer, A., He, D., & Just, N. (2023). The state is watching you – A cross-national comparison of data retention in Europe. *Telecommunications Policy*, 47(4), 102542. <https://doi.org/10.1016/j.telpol.2023.102542>
- Born, H., & Leigh, I. (2005). *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies*. Geneva Center for the Democratic Control of Armed Forces.
- Born, H., & Wills, A. (Eds.). (2013). *Overseeing intelligence services: An international study*. Geneva Center for the Democratic Control of Armed Forces.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.
- Carrington, K., Hogg, R., & Sozzo, M. (2016). Southern criminology. *British Journal of Criminology*, 56(1), 1–20. <https://doi.org/10.1093/bjc/azv083>
- Code de la sécurité intérieure [Internal Security Code], March 14, 2012. legifrance.gouv.fr
- Commission Nationale de Contrôle des Techniques de Renseignement. (2024). Huitième rapport d'activité 2023 [2023 Activity report]. https://cms.cnctr.fr/uploads/CNCTR_Rapport_2023_VERSION_NUMERIQUE_b1cd8eda21.pdf
- Connell, R. (2007). *Southern theory: The global dynamics of knowledge in social science*. Allen & Unwin.
- Council of Europe, European Commission for Democracy through Law (Venice Commission). (2015). *Report on democratic oversight of the security services* (CDL-AD(2015)010). [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=-CDL-AD\(2015\)010-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=-CDL-AD(2015)010-e)
- Csink, L. (2017). Mikor legyen a jogrend különleges? [When should the legal order be special?]. *Iustum Aequum Salutare*, 13(4), 7–16. https://ias.jak.ppke.hu/20174sz/01b_Csink_IAS_2017_4.pdf



- Csizner, Z. (2021). Az Emberi Jogok Európai Bíróságának titkos felderítést érintő ítélezési gyakorlata [The case law of the European Court of Human Rights concerning covert detection]. *Belügyi Szemle*, 69(4), 13–34. <https://doi.org/10.38146/BSZ.2021.4.9>
- Csizner, Z. (2024). A hatékonyság és törvényesség vizsgálata a titkos felderítés területén [Examining efficiency and legality in the field of covert detection] (PhD dissertation, NKE RTK). https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/0.%20Ertekezes_Csizner%20Zoltan.pdf
- Cucchiara, R., Baraldi, L., Cornia, M., & Sarto, S. (2024). Video surveillance and privacy: A solvable paradox? *Computer*, 57(3), 91–100. <https://doi.org/10.1109/MC.2023.3316696>
- European Commission. (2024). *Serbia Report 2024*. https://enlargement.ec.europa.eu/document/download/3c8c2d7f-bff7-44eb-b868-414730cc5902_en?filename=Serbia+Report+2024.pdf
- European Digital Rights. (2024). *EDRI's 2024 in review*. <https://edri.org/our-work/edris-2024-in-review/>
- European Parliament. (2023). *Briefing for the PEGA Committee mission to Hungary, 20–21 February 2023* (PE 752.601). Policy Department for Citizens' Rights and Constitutional Affairs. [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/752601/IPOL_STU\(2023\)752601_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/752601/IPOL_STU(2023)752601_EN.pdf)
- European Union Agency for Fundamental Rights. (2017). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU* (Vol. II). Publications Office of the European Union.
- European Union Agency for Fundamental Rights. (2022a). *National intelligence authorities and surveillance in the EU: France update*. https://fra.europa.eu/sites/default/files/fra_uploads/fr-surveillance-report-update-2022_en.pdf
- European Union Agency for Fundamental Rights. (2022b). *National intelligence authorities and surveillance in the EU: Hungary update*. https://fra.europa.eu/sites/default/files/fra_uploads/hu-surveillance-report-update-2022_en.pdf
- European Union Agency for Fundamental Rights. (2023). *Surveillance by intelligence services: 2023 update*. Publications Office of the European Union.
- Farkas, K. (2022). A leplezett eszközök alkalmazásának gyakorlati tapasztalatai [Practical experiences in the application of covert measures]. *Ügyészségi Szemle*, 7(2), 24–41.
- Finszter, G. (2024). A titkos eszközök alkalmazásának jogi alapjai [The legal foundations of the application of covert tools]. *Belügyi Szemle*, 72(6), 622–638. <https://doi.org/10.38146/BSZ-AJIA.2024.v72.i6.pp961-974>
- Fux, J., Haselbacher, M., & Reeger, E. (2023). Legislative responses to the BVT affair: Austria's intelligence service reform. *Intelligence and National Security*, 38(2), 201–218. <https://doi.org/10.1080/02684527.2022.2072454>
- Geneva Centre for Security Sector Governance. (2015). *Safeguards in electronic surveillance* (DCAF Parliamentary Brief). Geneva Center for the Democratic Control of Armed Forces.



Greene, D., & Rodriguez, K. (2014). *NSA mass surveillance programs: Unnecessary and disproportionate*. Electronic Frontier Foundation. https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf

Győri, A., & Szendrei, F. (2021). A leplezett eszközök alkalmazásának tapasztalatai a jogintézmény bevezetésétől napjainkig [Experiences in the application of covert measures from the introduction of the legal institution to the present day]. *Rendőrségi Tanulmányok*, 4(1), 72–92.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–620. <https://doi.org/10.1080/00071310020015280>

Horsley, J. P. (2019, September). Party leadership and the rule of law in the Xi Jinping era. *Brookings*. <https://www.brookings.edu/articles/party-leadership-and-rule-of-law-in-the-xi-jinping-era/>

Human Rights Watch. (2019, May 1). *China's algorithms of repression*. <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/>

Ilijevski, I., & Krstevska-Savovska, K. (2021). Control and supervision of the implementation of measures for interception of communications: The Macedonian case. *NBP. Nauka, bezbednost, policija*, 26(2), 43–52. <https://doi.org/10.5937/nabepo26-33542>

Jancsó, G. (2018). Leplezett eszközök alkalmazása: titkos információgyűjtés az új büntetőeljárási törvényben [Application of covert measures: secret intelligence gathering in the new Code of Criminal Procedure]. *Acta Humana*, (1), 19–34.

Krapac, D. (2010). Unlawful evidence in criminal procedure according to the case law of the European Court of Human Rights. *Zbornik Pravnog Fakulteta u Rijeci*, 31(1), 145–168.

Lazarus, L. (2021). Security and human rights. In B. J. Goold & L. Lazarus (Eds.), *Security and human rights* (2nd ed.) (pp. 1–24). Oxford University Press.

Liu, E. C. (2024). *The Foreign Intelligence Surveillance Act (FISA): An overview of selected issues* (CRS Report No. RL30465). Congressional Research Service.

Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions [Law no. 2023-380 of May 19, 2023 on the 2024 Olympic and Paralympic Games and introducing various other provisions], May 19, 2023. legifrance.gouv.fr

Lyon, D. (2004). *Globalizing surveillance*. University of Toronto Press.

Lyon, D. (2019). *The culture of surveillance: Watching as a way of life*. Polity Press.

Milosavljević, B. (2023). *Proposed solutions for improving the legal framework on the Serbian security and intelligence system*. Belgrade Centre for Security Policy.

National Authority for Data Protection and Freedom of Information. (2022). *Findings of the investigation of the Hungarian National Authority for Data Protection and Freedom of Information launched ex officio concerning the application of the Pegasus spyware in Hungary* (NAIH-423-2/2022).



- National People's Congress of the People's Republic of China. (2017). *National Intelligence Law of the People's Republic of China*. <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>
- National People's Congress of the People's Republic of China. (2021, August 20). *Personal Information Protection Law*. <https://personalinformationprotectionlaw.com/>
- Nyeste, P. (2012). A bűnügyi hírszerzés [Criminal intelligence]. *Magyar Rendészet*, 12(4), 22–37.
- Nyeste, P. (2018). A titkos információgyűjtés és a leplezett eszközök, a felderítés új modellje [Secret intelligence gathering and covert measures: the new model of detection]. *Belügyi Szemle*, 66(5), 14–30. <https://doi.org/10.38146/BSZ.2018.5.2>
- Nyeste, P., & Szendrei, F. (2019). *A bűnügyi hírszerzés kézikönyve* [Handbook of criminal intelligence]. Dialóg Campus.
- Oderkerk, M. (2025). Methods of comparative legal research: How to set up and carry out a comparative legal research project. In M. Bartl, L. Burgers, & C. Mak (Eds.), *Uncovering European private law: A student handbook* (pp. 311–342). Open Book Publishers. <https://doi.org/10.11647/OBP.0448.16>
- Pisarić, M. (2023). The use of policeware to hack electronic evidence in Germany and the Netherlands. *NBP. Nauka, bezbednost, policija*, 28(1), 16–26. <https://doi.org/10.5937/nabepo28-43759>
- Przeworski, A., & Teune, H. (1970). *The logic of comparative social inquiry*. Wiley-Interscience.
- Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, 126(7), 1934–1965.
- Saputra, E., & Handayani, F. (2024). The impact of digital surveillance on privacy rights: A legal and ethical analysis. *Proceeding of the International Conference on Law and Human Rights*, 1(2), 8–12. <https://doi.org/10.62383/iclehr.v1i2.22>
- Serbia's unregulated use of IMSI catchers raises concerns over privacy and civil liberties. (2024, December 12). *Serbia Business*. <https://serbia-business.eu/serbias-unregulated-use-of-imsi-catchers-raises-concerns-over-privacy-and-civil-liberties/>
- Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.
- Steiner, G. (2021). A bírói engedélyhez kötött leplezett eszköz és a titkos információgyűjtés eredményének felhasználása [The use of judicially authorised covert measures and the results of secret intelligence gathering]. *Magyar Rendészet*, (4), 171–187. <https://doi.org/10.32577/mr.2021.4.9>
- Steiner, G. (2023). A bírói engedélyhez kötött leplezett eszközök hatályos szabályozásának önellentmondásai és módosítási javaslatok [Internal contradictions in the current regulation of judicially authorised covert measures, and proposals for amendment]. *Belügyi Szemle*, 71(2), 221–237. <https://doi.org/10.38146/BSZ.2023.2.3>



Šurlan, T. (2021). The duty to protect the right to life. *NBP. Nauka, bezbednost, policija*, 26(2), 19–30. <https://doi.org/10.5937/nabepo26-34101>

Turanjanin, V. (2022). Special investigative measures: Comparison of the Serbian Criminal Procedure Code with the European Court of Human Rights standards. *International Journal of Evidence & Proof*, 26(1), 44–65. <https://doi.org/10.1177/13657127211055230>

Weber, M. (1949). *The methodology of the social sciences*. Free Press.

Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske [Act on the Security and Intelligence System of the Republic of Croatia], *Narodne novine*, 79/2006 and 105/2006 (corrigendum). <https://www.zakon.hr/z/744>

Zekavica, R. G. (2019). The rule of law in the function of human dignity. *NBP. Nauka, bezbednost, policija*, 24(2), 17–28. <https://doi.org/10.5937/nabepo24-21119>

Živanović, K. (2018). Secret surveillance of communication as special evidence: The practice of the European Court of Human Rights in the case of a non-reasoned court order. *NBP. Nauka, bezbednost, policija*, 23(3), 287–310. <https://doi.org/10.5937/nabepo23-18350>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

ONLINE FIRST

