Journal of Criminology and Criminal Law, 64(1), 103-123
Review paper
https://doi.org/10.47152/rkkp.64.1.6
UDK: 343.14/.15
342.738
341.231.14(4)

RECEIVED: 11 January 2026
ACCEPTED: 19 March 2026

The Strasbourg Standards of Mass Surveillance of Communications

Miloš Biberdžić[a]

This paper examines the standards governing mass surveillance of communications under the European Convention on Human Rights (ECHR), as developed in the jurisprudence of the European Court of Human Rights (ECtHR). It aims to identify, analyse, and systematise the Strasbourg standards binding the Contracting States in regulating mass surveillance of communications under the ECHR. The central research question is whether the Strasbourg case law provides a coherent and operational framework capable of reconciling national security imperatives with the effective protection of fundamental rights and freedoms. The analysis proceeds from doctrinal scholarship on mass surveillance, through an interpretative reading of the Convention, to a systematic assessment of the ECtHR's jurisprudence, with cases selected for their role in shaping the scope, limits, and safeguards of bulk interception. The paper demonstrates that, under the ECHR, the ECtHR permits mass surveillance only conditionally and subject to strict safeguards. The analysis identifies five cumulative Strasbourg standards, articulated through corresponding safeguards, that structure the assessment of mass surveillance under the European Convention on Human Rights: legality, independent oversight, data protection safeguards, proportionality, and effective remedies. Rather than operating as isolated requirements, these standards function as interdependent elements of a coherent framework.

KEYWORDS: mass surveillance, bulk interception, Strasbourg standards, data protection safeguards, proportionality, European Convention on Human Rights, chilling effect

[a] PhD student, Faculty of Law, University of Belgrade. E-mail: milos.biberdzic@gmail.com.

Introduction

Mass (or bulk) surveillance[1] involves the large-scale interception and analysis of telephone and internet communications, often encompassing individuals who are not under any reasonable suspicion of criminal activity. It is proactive, aiming to identify potential risks, and therefore employed by intelligence agencies as a tool to safeguard national security. However, due to its broad scope, lack of proportionality, and indiscriminate nature, mass surveillance may also pose a serious threat to human rights and civil liberties.

The collection of data through mass surveillance can profoundly affect the relationship between citizens and the state. An imbalance in access to information may tip the scales of power, limiting citizens' ability to exercise democratic oversight and hold accountable those elected to represent them (Forcese and Freeman, 2011, pp. 481–484, as cited in Newell, 2014, p. 482). To address this inevitable asymmetry of power, it is necessary to develop legal frameworks that ensure the effective protection of human rights. The distinction between democratic and autocratic systems rests largely on how the state perceives its citizens: as trusted rights-holders or as potential suspects (Bernal, 2016, p. 259). This tension between trust and suspicion is particularly visible in the digital age, where the use of mass surveillance has made repression more efficient and enabled authoritarian regimes to consolidate control through selective and data-driven means (Xu, 2021).

In Europe, mass surveillance practices have often evolved within a constitutional vacuum, allowing executive authorities to expand their powers even after global disclosures of extensive rights violations (Celeste and Formici, 2024, pp. 428-429). To prevent a threat to collective security from being replaced by the threat of excessive surveillance carried out by unchecked executive power and to ensure the protection of human rights, legislation must timely keep pace with developments in digital technologies and remain consistent with international human rights instruments. Mass surveillance must be regulated within national legal systems in full compliance with international treaties that guarantee human rights.

The European Convention on Human Rights (hereinafter: ECHR) represents the most significant regional human rights instrument of this kind, binding nearly all European states.[2] Its provisions are largely abstract, functioning as guiding legal principles. Therefore, understanding and interpreting them requires familiarity with the case law of the European Court of Human Rights in Strasbourg (hereinafter: ECtHR), which has, through its judgments, given them substantive content and true meaning (Beširević *et al*., 2017, p. 14).

This paper aims to systematize and critically assess the Strasbourg standards governing mass surveillance of communications, identifying the safeguards required for its

[1] The term *bulk surveillance* is often used in academic writing and recent ECtHR case law (e.g. *Big Brother Watch and Others v. UK* [GC]) to describe the large-scale, indiscriminate interception of communications data, while earlier judgments, such as *Weber and Saravia v. Germany*, referred to *strategic surveillance*. In this paper, however, the term *mass surveillance* is preferred for its clarity and broader recognition in both legal and public discourse.

[2] With the notable exceptions of the Vatican City State and Belarus.

legitimacy. The central research question asks whether the jurisprudence of the ECtHR provides a coherent and predictable framework for reconciling mass surveillance with the protection of fundamental rights. Methodologically, the paper proceeds from a doctrinal analysis of contemporary legal scholarship, through a normative interpretation of the relevant Convention provisions, to a jurisprudential examination of the ECtHR's case law. The study focuses on landmark ECtHR cases concerning bulk interception, selected for their precedential value and contribution to the development of safeguards. Against this background, the following chapter introduces the key conceptual foundations and normative assumptions underlying mass surveillance of communications.

The Specificities of Mass Surveillance

A precise understanding of the distinction between mass and targeted surveillance, the legal significance of metadata in relation to the content of communications, and the role of effectiveness of bulk interception of communications is essential for a doctrinal analysis of mass surveillance.

Mass Surveillance and Targeted Surveillance: A Normative Distinction

Mass surveillance of communications typically involves the large-scale interception, storage, and algorithmic processing of data transmitted via telephone or internet networks. Such operations are generally conducted by intelligence services without individualized suspicion or prior judicial authorisation (Slobogin, 2015, pp. 518, 522). Their proclaimed objective is to protect national security by identifying emerging threats through the analysis of communication patterns rather than content.

In contrast, targeted surveillance refers to the interception of communications based on prior judicial authorisation and the existence of procedurally relevant degree of suspicion that a specific individual or group is involved in criminal activity. Its primary purpose is the collection of evidence within a framework of procedural safeguards that ensure judicial oversight, necessity assessment, and proportionality control. Unlike mass surveillance, it operates on a case-by-case basis and presupposes a concrete link between the person monitored and a legitimate investigative purpose.

The distinction between mass and targeted surveillance is therefore not merely technical but normative. Targeted interception is anchored in individualized suspicion and judicial oversight. Mass surveillance, by contrast, may treat all individuals as potential subjects of monitoring and relies on institutional safeguards rather than personalized suspicion. Accordingly, its legitimacy under the Strasbourg framework depends on whether states can demonstrate that bulk interception regimes are governed by strict and effective safeguards derived from, yet adapted beyond, those applied in targeted surveillance.

Metadata and the Content of Communications: Conceptual and Normative Significance

Another central conceptual distinction concerns the differentiation between the content of communications and metadata. Content refers to the essence of communications, such as text, a photo and video message, or an audio recording of a conversation. The information collected through bulk interception consists primarily of metadata - data generated automatically whenever a digital device is used. Metadata is often described as "data about data" (Newell, 2014, pp. 487-488), and includes information such as the identities of communicating parties, the time, duration, and frequency of interactions, as well as geolocation and device identifiers. While metadata does not reveal the substantive content of communications, it can nevertheless disclose extensive information about an individual's private life. Contrary to the assumption that metadata represents a lesser intrusion, scholars have emphasized that it can, in many contexts, be more revealing than content itself (Bernal, 2018, p. 176). Metadata analysis enables intelligence agencies to map social networks, infer personal relationships, and construct detailed behavioural profiles. Whether based on data from law enforcement and security agencies or on automated analysis, algorithmic surveillance creates categories of individuals, sometimes with no obvious connection, whose rights still require protection (Kosta, 2020, p. 213). Through algorithmic processing, individuals may be categorized along political, ethnic, or religious lines, raising concerns over compliance with human rights standards.

From an operational perspective, metadata is often preferred to content data. It can be processed automatically by software or artificial intelligence, whereas content analysis usually requires human interpretation. Moreover, content may be protected by encryption or coded language, while metadata, as a by-product of device usage, is almost impossible to conceal (Bernal, 2018, p. 176). This makes metadata both more precise and more reliable as a tool for surveillance, but also more intrusive in its implications for privacy and autonomy.

This distinction is therefore normatively relevant not because metadata is inherently less sensitive than content, but because its large-scale collection and analysis can generate comparable, and in some contexts even greater, interferences with individual rights.

Assessing the Effectiveness of Mass Surveillance

One of the most frequently invoked arguments in favour of mass surveillance is its effectiveness in preventing terrorism, serious crime, and threats to national security. Effectiveness is often presented as a self-evident justification, grounded in the assumption that broader data collection enhances the ability of authorities to detect unknown threats. However, from a normative perspective, effectiveness cannot function as an autonomous or conclusive justification. Broader data collection does not necessarily correlate with increased public safety, for at least two reasons. First, intelligence agencies may face analytical overload, reducing the efficiency of targeted surveillance measures that have proven operationally effective. Second, increased surveillance may fuel public interest in protecting privacy, prompting wider use of encrypted communications. Consequently, some states have intro-

duced lawful hacking powers to bypass encryption, raising important concerns regarding privacy protection and the security of information systems (Pisarić, 2022, pp. 70-71).

Some official reports point to benefits of bulk surveillance such as network mapping, pattern recognition, resource efficiencies, and retrospective analysis (Murray and Fussey, 2019, pp. 36-43). Yet, critics argue that expanding data collection may only deepen inefficiency. A commonly used metaphor for mass surveillance is "searching for a needle in a haystack" (Richards, 2019; Logan, 2017), and building a bigger haystack, they contend, only makes the needle harder to find.[3]

This critique underlines a central normative dilemma: whether extensive data collection genuinely contributes to security or merely amplifies the risks of overreach, arbitrariness, and rights violations. The answer, as reflected in the Strasbourg Court's jurisprudence, which will be examined in greater detail in the following chapters, does not rest on the scope of surveillance itself, but on the quality of the legal framework and the effectiveness of institutional safeguards designed to prevent abuse and ensure accountability.

Mass Surveillance through the Lens of the ECHR: Legal Framework and Affected Rights

Before examining the standards developed in the jurisprudence of the European Court of Human Rights, this chapter sets out the Convention framework governing mass surveillance of communications. It identifies the Convention rights most directly affected by large-scale interception and analyses key judgments illustrating how such practices interfere with their effective enjoyment.

The ECtHR's Four-Stage Framework for Assessing Interference with Convention Rights in Mass Surveillance

The ECtHR has accepted the establishment of mass surveillance systems for the purpose of protecting national security, but only if adequate and effective safeguards are in place to prevent abuse. Without such safeguards, there is a risk that, under the pretext of national security, democratic processes may be undermined (*Big Brother Watch and Others v. UK* [GC], § 339; *Centrum för rättvisa v. Sweden* [GC], § 253). The Court has emphasized that mass surveillance is not inherently less intrusive than targeted surveillance. Intercepted and retained metadata must be afforded the same level of protection as communication content (*Ekimdzhiev and Others v. Bulgaria*, § 394).

According to the ECtHR, mass surveillance is a gradual process in which the degree of interference with human rights increases as the process advances. The Court identifies four distinct phases (*Big Brother Watch and Others v. UK* [GC], §§ 325-329*; Centrum för rättvisa v. Sweden* [GC], §§ 239-243):

[3] Joint Committee on the Draft Investigatory Powers Bill (2016).

Interception Phase: Intelligence agencies intercept electronic communications involving a large number of individuals, the overwhelming majority of whom are not of interest. Filtering at this stage is minimal or absent.

Initial Search Phase: The data is subjected to preliminary searches using strong selectors (e.g., specific email addresses) and/or complex search queries to identify relevant individuals.

Analytical Phase: Selected communications are examined by analysts for the first time.

Utilization Phase: Intelligence services make use of the intercepted material, typically by producing intelligence reports, which may be shared with other domestic or foreign security services.

Considered jointly, these four stages illustrate a structured model of state interference, in which each subsequent phase entails a progressively deeper intrusion into individual rights and therefore requires correspondingly stricter legal safeguards.

Mass Surveillance as a Multi-Rights Interference under the ECHR

Mass surveillance can be indiscriminate, potentially affecting both individuals who may give rise to reasonable suspicion and those who do not. It can also be disproportionate, insofar as it may impose significant burdens on individuals and society relative to the security benefits achieved (Macnish, 2020, p. 2).

While the primary implications of mass communication surveillance may concern the right to respect for private and family life, its effects on the right to a fair trial, freedom of thought, conscience, and religion, freedom of expression, freedom of assembly and association, and the prohibition of discrimination must not be overlooked. A narrow focus solely on the right to privacy may lead to an incomplete understanding of the broader risks posed by bulk surveillance, not only for individuals, but also for democratic society. Moreover, such a limited perspective may result in the application of unduly lenient standards when assessing the legitimacy and lawfulness of surveillance measures (Bernal, 2016, p. 252).

Interference with the Right to Respect for Private and Family Life (Article 8 ECHR)

Mass surveillance raises issues under Article 8 of the Convention due to its capacity to enable systematic access to information concerning individuals' private and family life. The ECtHR has consistently held that the right to respect for private life and correspondence under the ECHR encompasses postal, telephone, and email communications (*Kennedy v. the United Kingdom*, § 118), as well as internet searches, even when conducted from a workplace (*Copland v. the United Kingdom*, § 41). The concept of "correspondence" must be interpreted in light of technological developments, meaning that all modern forms of electronic communication, such as Viber, WhatsApp, Telegram, Signal and similar services, should fall within the protective scope of Article 8.

Examining mass surveillance exclusively from the perspective of correspondence could, however, be an unjustified simplification for two reasons. First, there is significant

overlap between the right to correspondence and the rights to private life, family life, and home, making it difficult to identify which specific aspect of Article 8 has been infringed. In particular, bulk surveillance represents both an interference with private life and a violation of the confidentiality of correspondence. Second, mass surveillance potentially interferes more deeply with private and family life than with correspondence, given that nearly all aspects of modern private life are directly or indirectly exposed online. From the standpoint of legitimacy, the crucial question is not whether the information is private, but how it is collected, analysed, and for what purpose. While the right to respect for private life is not absolute, any restriction must comply with the strict safeguards prescribed by the Convention. States are under a negative obligation to refrain from unlawful interference and a positive obligation to ensure the effective enjoyment of this right, subject to the strict conditions laid down in the Convention.

Interference with the Right to a Fair Trial (Article 6 ECHR)

The right to a fair trial constitutes one of the most fundamental procedural safeguards, providing effective protection for other rights that underpin individual freedoms (Ilić, 2011, p. 229). Mass surveillance of communications may affect this right in multiple ways.

The presumption of innocence, a cornerstone of fair trial guarantees, can be undermined by mass surveillance. Its broad, indiscriminate scope may foster a social climate in which individuals are treated as suspects before there is any legally threshold of suspicion. The presumption of innocence is closely linked to the duty of impartiality, which itself is a prerequisite for ensuring the equality of arms between the parties (Miljuš, 2021, p. 86).

Mass surveillance may compromise the confidentiality of communication between clients and legal counsel, interfering with the right to an adequate defence. The essential role of lawyers would be undermined if client communications could not remain confidential (*Michaud v. France*, § 118).

In cases where surveillance measures do not meet statutory standards, questions may arise regarding the admissibility of evidence obtained through such means. The ECtHR has not established comprehensive rules on evidence admissibility nor rigid standards for evidence assessment.[4] In general, the admissibility and evaluation of evidence, including material derived from secret surveillance measures, remains primarily governed by domestic law and determined by national courts (Ilić, 2021, p. 124). The Court's role is not to act as a final court of fourth instance, but to assess whether the proceedings as a whole, including the manner in which evidence was obtained, were fair (*Jalloh v. Germany* [GC], § 95). Its function is primarily supervisory, occasionally corrective, and only rarely directive (Dajović and Spaić, 2019, p. 182). This could be particularly relevant in cases of bulk surveillance, where individuals may be unable to identify whether, and to what extent, intercepted material has been used against them in criminal proceedings.

[4] The only absolute exception concerns evidence obtained through torture, which is inadmissible under all circumstances (Ilić, 2015, p. 80).

Interference with Freedom of Thought, Conscience and Religion (Article 9 ECHR)

Individuals may be deterred from freely expressing their views or religious beliefs when they are aware that their communications may be subject to mass surveillance. This phenomenon, commonly referred to as the *chilling effect*, can suppress free expression by instilling fear of state scrutiny. Studies indicate that human behaviour changes when we know we are being observed, leading us to act less freely, which in effect means we are less free.[5] Pervasive surveillance and the analysis of intercepted information may amplify the influence of powerful social actors, such as security agencies, in shaping individuals' choices and actions (Nissenbaum, 2009, p. 83).

Mass surveillance that disproportionately targets specific groups may lead to self-censorship, the homogenization of thought and belief, and ultimately undermine the principles of pluralism of opinion and freedom of religion. If directed at religious institutions, such surveillance can also impair their autonomy and freedom to operate independently. In *Miroļubovs and Others v. Latvia*, the Court emphasized that state interference in the internal affairs of a religious community, including through measures of oversight and control, can violate the right to freedom of religion (§§ 80–82).

Interference with Freedom of Expression (Article 10 ECHR)

The chilling effect also extends to the freedom of expression. Awareness of being under surveillance may create a societal climate in which individuals hesitate to express their opinions freely, fearing repercussions. Mass surveillance can identify and track individuals or groups expressing dissent, thereby suppressing opposing views and undermining the free exchange of ideas.

Bulk surveillance can also compromise anonymity, vital for expressing unpopular opinions without retaliation. Journalists may self-censor if they fear state monitoring, undermining press freedom, particularly when sources and communications are insufficiently protected (*Big Brother Watch and Others v. UK* [GC], §§ 447–450).

Freedom of expression underpins whistleblower protection, which is necessary to preserve the transparent and accountable functioning of institutions, especially where secrecy surrounding mass surveillance limits public scrutiny. Whistleblowers are entitled to protection under Article 10 when disclosing information in the public interest.[6]

Interference with Freedom of Assembly and Association (Article 11 ECHR)

Freedom of peaceful assembly is a cornerstone of democracy and must not be interpreted restrictively (*Djavit An v. Turkey*, § 56). Mass surveillance tools can monitor groups regardless of unlawful activity, creating a chilling effect on the exercise of free-

[5] Snowden, J. (2014) *Snowden Answers Our Burning Data Collection Question: What's the Worst That Could Happen?* Available at: https://techcrunch.com/2014/01/23/snowden-answers-our-burning-data-collection-question-whats-the-worst-that-could-happen/ (Accessed: 01 September 2025)

[6] The ECtHR has rightly recognised that, in certain circumstances, the public interest may outweigh the confidentiality obligations imposed on civil servants (*Guja v. Moldova* [GC], §§ 70–73).

dom of assembly and association. The ECtHR in the case of *Glukhin v. Russia* illustrates the chilling effect that mass surveillance may have on the right to freedom of assembly, especially when combined with emerging technologies such as facial recognition. The Court emphasized that indiscriminate surveillance of peaceful protestors, particularly through facial recognition, fails to satisfy the Convention safeguards (§§ 86–89). Freedom of assembly is especially significant for minorities, who rely on it to express cultural identity and protect collective rights (*Gorzelik and Others v. Poland*, § 93).

Interference with Prohibition of Discrimination (Article 14 ECHR)

Rights under the ECHR must be secured without discrimination. Mass surveillance can generate large datasets, which, when analysed automatically, may classify individuals along protected characteristics (sex, race, colour, language, religion, political opinion, national or social origin, minority status, property, birth, or other status), potentially resulting in discriminatory profiling. Selective or disproportionate targeting based on these characteristics constitutes discrimination if it lacks objective and reasonable justification. Discrimination arises where the measure fails to pursue a legitimate aim or where the means are not proportionate to the aim. (*Okpisz v. Germany*, § 33). States enjoy a margin of appreciation regarding differentiation in otherwise similar situations. Large-scale data collection, notwithstanding the exercise of substantial caution, may still produce discriminatory effects through the inadvertent reliance on variables that are correlated with protected groups (Barocas & Selbst, 2016, p. 675).

Mass surveillance is particularly prone to resulting in indirect discrimination, which occurs when a seemingly neutral measure or policy has a disproportionately negative impact on a particular individual or group (Beširević *et al*., 2017, p. 364).

Considered jointly, these dimensions illustrate that mass surveillance can threaten not only the privacy of individuals but the institutional integrity. The Strasbourg approach therefore treats surveillance as a multi-rights issue, demanding systemic safeguards rather than *ad hoc* justification. The next chapter explores how the Court has articulated these safeguards through its evolving standards of legality, independent oversight, data protection safeguards, proportionality and effective remedies.

Strasbourg Standards Governing Mass Surveillance - An Analysis of the ECtHR's Jurisprudence under the ECHR –

The European Court of Human Rights has consistently emphasized that the rights guaranteed by the European Convention on Human Rights must be practical and effective, rather than theoretical or illusory (*Airey v. Ireland*, § 24). In the field of communications surveillance, this principle requires that national legal frameworks clearly reflect the Convention's requirements as interpreted by the Court. These standards are shaped both by the text of the ECHR and by the Court's case law, which together constitute *European human rights law* (Popović, 2011, p. 344).

The Strasbourg Court has repeatedly underlined that bulk interception of communications may represent interference with fundamental rights and therefore demands strict justification and robust procedural safeguards. On the basis of an analysis of the ECtHR's jurisprudence, the following cumulative standards may be identified: legality, independent oversight mechanisms, data protection safeguards, proportionality and availability of effective legal remedies. These standards function as safeguards against arbitrariness and abuse and must be cumulative fulfilled for mass surveillance to comply with the Convention.

Although these safeguards are examined separately for analytical clarity, the Court's case-law treats them as interdependent and mutually reinforcing, making some overlaps inevitable in their analysis in this paper. The following sections examine these standards in the way in which the ECtHR applies them to assess the compatibility of mass surveillance regimes with the Convention, concluding with cases that illustrate the increasingly blurred line between targeted and bulk interception, particularly in the monitoring of encrypted communications.

Legality as a Structural Safeguard in Mass Surveillance

A core element of legality in Strasbourg jurisprudence is foreseeability. The laws,[7] including those governing mass interception regimes, must be formulated with sufficient clarity to enable individuals to foresee the consequences of their actions and understand potential sanctions (*Kafkaris v. Cyprus* [GC], § 140). This does not require predicting specific interception instances, but it does demand clear criteria for when and under what conditions surveillance may occur (*Malone v. the United Kingdom*, § 67; *Weber and Saravia v. Germany*, § 93). Foreseeability does not necessitate an exhaustive enumeration of offences that may justify targeted interception. Laws should define categories of offences and persons subject to surveillance (*Kennedy v. the UK*, § 159). Vague or overly broad legislation fails this standard (*Iordachi and Others v. Moldova*, § 41). Bulk surveillance laws cannot be too detailed or too concrete, because the whole power of such surveillance relies on the use of flexible algorithms (Kosta, 2020, p. 220). However, warrants should define categories of selectors (*Big Brother Watch and Others v. UK* [GC], §§ 351–352; *Centrum för rättvisa v. Sweden* [GC], §§ 265–266). When selectors relate to identifiable individuals, heightened safeguards are required (*Big Brother Watch and Others v. UK* [GC], § 355; *Centrum för rättvisa*, § 269). Particular attention should be given to *contact chaining*, a technique for identifying individuals connected to a surveillance target through metadata analysis. As it risks extending surveillance beyond the original target, the law must clearly define its permissible scope, including limits on the number of "hops" and criteria for querying bulk data (Watt, 2017, p. 788). While foreseeability remains a key element of legality, in the field of mass surveillance its role has been partially reinterpreted. As mass surveillance is inherently secret, the ECtHR has shifted its focus from individual predictability toward structural safeguards capable of preventing abuse (Van der Sloot, 2020).

Accessibility is another integral element of the legality requirement, and ensures that the legal framework governing surveillance is open to public scrutiny. This requires that

[7] The ECtHR interprets "law" broadly, encompassing statutes, subordinate legislation, judicial practice (*Sunday Times v. the UK*, § 47), and even unwritten law (*Kafkaris v. Cyprus* [GC], § 139).

surveillance laws be publicly available, published online, and adopted by the legislature before entering into force (*Kennedy v. the UK*, § 157).

The Court's approach to legality was further clarified in the twin Grand Chamber judgments of *Big Brother Watch and Others v. the UK* and *Centrum för rättvisa v. Sweden*, where it affirmed that bulk interception may be compatible with the Convention, provided that strict safeguards are in place. These safeguards build upon the criteria first developed in *Roman Zakharov v. Russia* [GC], where the Court found that an abstract review of surveillance law was justified given its secret nature, broad scope, and lack of effective remedies. The Court held that the mere existence of a legal framework permitting secret surveillance, if it fails to provide adequate safeguards, may in itself amount to a violation of the Convention (§ 178).

Although the ECtHR's review in these cases has primarily been in abstracto due to the secrecy surrounding surveillance operations, the principle of legality remains the cornerstone of Convention-compatible surveillance, ensuring that state power is exercised within clearly defined limits. However, the availability of abstract scrutiny of mass surveillance does not by itself guarantee stronger protection of privacy in practice, as the ECtHR has been criticized for the limited enforceability of its judgments (Carpenter, 2021, p. 54). The Strasbourg Court acknowledges that legislation is drafted for general application and that legislative technique cannot achieve absolute precision. It therefore allows national courts to interpret laws in line with societal needs (Kononov v. Latvia [GC], § 185), while refraining from reviewing such interpretations unless there is flagrant non-observance or arbitrariness (Huhtamäki v. Finland, § 52). Overall, the Court's approach suggests that legality in mass surveillance functions primarily as a structural safeguard for organizing and reviewing surveillance powers.

Independent Oversight as a Constraint on Executive Discretion

To establish adequate and effective safeguards against abuse, it is essential to ensure independent oversight of the operation of mass surveillance regimes (*Weber and Saravia v. Germany*, § 117). The decisive criterion in assessing an oversight body is not its formal designation as a court or administrative authority, but the existence of substantive guarantees of independence and impartiality. Such guarantees include autonomy from the executive, objective and transparent procedures for the appointment and tenure of members, and effective protection against external influence or pressure (Mitsilegas *et al*., 2021, p. 197). In its jurisprudence, the ECtHR has developed two main models of oversight: judicial and non-judicial.

Judicial oversight provides the strongest guarantees of impartiality and independence. The rule of law requires the existence of an effective judicial system capable of providing redress in cases of violations of human rights and fundamental freedoms (Ilić, 2021, p. 120). Even in the context of espionage or counter-terrorism, states cannot exercise unfettered discretion to monitor individuals (*Klass and Others v. Germany*, §§ 48, 55). Accordingly, restrictions on the rights of citizens must remain subject to judicial review, which serves as a benchmark for the effectiveness of protective mechanisms internationally (Ilić, 2011, p. 228).

Non-judicial oversight can also provide effective protection, provided that the bodies entrusted with such tasks are vested with the competence and authority to exercise meaningful control (*Leander v. Sweden*). While prior judicial authorisation is an important safeguard, it is not absolute; bulk interception may be authorised by independent of the executive (*Big Brother Watch and Others v. UK* [GC], § 351; *Centrum för rättvisa v. Sweden* [GC], § 265). To prevent abuse, an independent authority should be informed of the purpose of the interception, targets, communication channels involved, including the choice of selectors (*Big Brother Watch and Others v. UK* [GC], § 352; *Centrum för rättvisa v. Sweden* [GC], § 266). The Court requires end-to-end safeguards, encompassing prior authorisation by an independent authority, continuous supervision, and *ex post facto* review of completed operations (*Big Brother Watch and Others v. UK* [GC], § 361; *Centrum för rättvisa v. Sweden* [GC], § 264).

Taken together, these requirements indicate that independent oversight functions as a structural constraint on executive discretion, ensuring that surveillance powers remain subject to ongoing institutional control.

Data Protection Safeguards as a Limitation on Data Use and Retention

Data protection constitutes a regulatory framework establishing a coherent set of rules and principles governing all forms of personal data processing, irrespective of whether such processing is carried out by automated means or otherwise (Lynskey, 2023, pp. 300, 302). In the context of mass surveillance, it requires that individuals be duly informed about the collection, processing, and storage of their personal data, and that appropriate safeguards ensure the preservation of privacy and data security. In *Rotaru v. Romania* the Court broadened the notion of "surveillance" to include the systematic collection and retention of personal data, even where the information is publicly available (§§ 43, 46).

The Strasbourg Court has articulated three core standards concerning data protection safeguards in the context of bulk surveillance activities. First, data may only be used for the purposes for which they were collected. Second, the possibility of sharing the collected data with other state authorities must be strictly limited. Third, personal data must be stored securely and destroyed once they are no longer necessary for the pursuit of a legitimate aim (*Weber and Saravia v. Germany*, § 116). When assessing the handling of material obtained through targeted interception, the Court has further held that the law should strictly limit the number of persons to whom such material may be disclosed, require an appropriate level of security clearance for those with access, and prescribe that disclosure should occur only on a "need-to-know" basis (*Kennedy v. the UK*, § 163).

Recent judgments, such as *Pietrzak and Bychawska-Siniarska and Others v. Poland*, reiterated that the widespread retention of communications data by service providers, and their subsequent processing by the authorities, must be accompanied, *mutatis mutandis*, by safeguards and protective measures against abuse comparable to those applicable to targeted secret surveillance (§ 250). The Court observed that retained metadata enable the creation of an "intimate portrait" (*un portrait intime*) of the person concerned, revealing

social interactions, movements, browsing habits, and communication patterns, and therefore amount to an interference with the individual's private sphere (§ 253). More recently, the ECtHR emphasized in *Podchasov v. Russia* that the mere existence of laws requiring service providers to decrypt end-to-end encrypted communications, without any individualized suspicion or prior justification, constitutes a disproportionate interference that compromises user security and violates the right to respect for private life.

As mass surveillance often involves transnational data exchange, the absence of clear international rules on cross-border transfer and use of intercepted data creates an additional challenge. Without such regulation, states may indirectly circumvent domestic restrictions, weakening both accountability and the protection of individual rights. In this regard, the *Big Brother Watch* Grand Chamber judgment represents a pivotal development, as it was the first to address international intelligence sharing under the Convention. The Court adopted a cautious and deferential stance, accepting that states may exchange information obtained through mass surveillance provided that adequate safeguards are effectively implemented (Zalnieriute, 2022).

In this sense, Court's jurisprudence suggests that data protection safeguards in the context of mass surveillance function as limitation on the use, retention, and circulation of intercepted data, rather than as a barrier to data collection as such.

Proportionality in Bulk Interception Regimes

According to the principle of proportionality, derogations and limitations on the protection of human rights must be applied only to the extent that they are strictly necessary and accompanied by minimum safeguards providing individuals with sufficient guarantees to effectively protect their rights against abuse (Vogiatzoglou, 2019). However, mass surveillance is by its very nature difficult to reconcile with this principle, as it involves the collection of data whose necessity cannot be demonstrated, or even assessed, prior to their acquisition (Rojszczak, 2021, p. 57). In the context of mass surveillance, proportionality therefore requires that any measure be both necessary and proportionate with the legitimate aim pursued. Where such measures exceed what is required to address the threat at issue, they risk undermining fundamental rights through excessive monitoring. The Strasbourg Court found a system of targeted surveillance to be "excessively used" where domestic courts had granted virtually all prosecutorial requests for interception warrants over a three-year period (*Iordachi and Others v. Moldova*, § 52).

Legislation permitting secret monitoring may be necessary and proportionate when aimed at safeguarding national security and preventing crime (*Weber and Saravia v. Germany*, § 148). States are therefore required to assess necessity and proportionality at every stage of a bulk surveillance operation (*Big Brother Watch and Others v. UK* [GC], § 350). When assessing proportionality, states enjoy a margin of appreciation in determining whether interferences with individual rights are necessary to protect national security (*Weber and Saravia v. Germany*, § 106). This margin rests on the premise that national authorities are better placed to evaluate how Convention provisions are to be

applied within their domestic legal systems (Popović, 2008, p. 110). However, given that broad discretion in the conduct of bulk surveillance may *ab initi*o compromise proportionality, strict compliance with the other Strasbourg standards remains indispensable.

The proportionality requirement also mandates that the law clearly define the maximum duration of surveillance measures and the conditions for their extension. Targeted interception should be limited in time; extensions may be granted only upon a fresh request that complies with statutory conditions. Once the grounds for surveillance no longer exist, the measure must be terminated without delay (*Weber and Saravia v. Germany*, § 116). Although these temporal safeguards were initially formulated in the context of targeted interception, they are equally applicable to bulk surveillance, where the risks of prolonged and disproportionate interference with privacy are even greater. The ECtHR confirmed this approach emphasizing that the same fundamental safeguards, including strict temporal limits, must govern both targeted and bulk interception (*Big Brother Watch and Others v. the UK* [GC], §§ 314–317). Some flexibility may be permitted, depending on the complexity of an investigation, but only if adequate procedural and institutional safeguards are in place (*Kennedy v. UK*, § 161). In assessing proportionality, the Court also considers the fairness of the procedure, the availability of less intrusive means to achieve the legitimate aim, the existence of a pressing social need, and the extent to which the essence of the right was impaired (Paunović and Carić, 2006, p. 20).

Overall, the ECtHR's approach indicates that proportionality in mass surveillance extends beyond the initial authorization and depends on the combined operation of temporal limits and procedural guarantees.

The Right to an Effective Remedy

Everyone whose rights and freedoms guaranteed by the ECHR have been violated is entitled to an effective remedy before national authorities, even where the interference results from acts of public officials performed in an official capacity, including in the context of mass surveillance.

A defining feature of both mass and targeted surveillance is secrecy. Since the effectiveness of such measures depends on confidentiality, the ECtHR has held that a remedy must be available once the existence of secret measures is disclosed to the individual concerned (*Segerstedt-Wiberg and Others v. Sweden*, § 117). In this field as well, the Court has developed a set of general safeguards applicable to mass surveillance.

The Court requires that the totality of remedies under domestic law be effective (*Leander v. Sweden*, § 77). Several individually ineffective remedies cannot cumulatively amount to one effective remedy (*Leander v. Sweden, partly dissenting opinion of judges Pettiti and Russo*). A constitutional complaint may also qualify as an effective remedy (*Marinković v. Serbia*, § 59), making its use a necessary precondition for access to Strasbourg.

An effective remedy must be capable of rectifying an alleged violation and offer a reasonable prospect of success, without requiring certainty of a favourable outcome (*Lorse and Others v. Netherlands*, § 96). Remedies cannot exist merely in abstract terms; they

must also function effectively in practice, and it is for the state to demonstrate this (*Iovchev v. Bulgaria*, § 142).

Importantly, in the context of bulk interception, the Court has recognised that remedies not dependent on notification of the subject may still be effective and may even provide stronger safeguards than systems that rely on *ex post facto* notification (*Big Brother Watch and Others v. UK* [GC], § 358; *Centrum för rättvisa v. Sweden* [GC], § 272).

The Court's jurisprudence indicates that the right to an effective remedy in the context of mass surveillance is primarily ensured through the existence of institutional mechanisms capable of independent review and correction, rather than through individual notification and participation. In this sense, the right to an effective remedy completes the system of Strasbourg safeguards by linking legality, oversight, data protection, and proportionality to mechanisms of review and accountability.

Viewed together, these standards form a coherent legal framework through which the ECtHR assesses the legitimacy of mass interception regimes. Yet, as technology evolves and surveillance techniques grow more sophisticated, the distinction between targeted and bulk interception becomes harder to sustain in practice, as illustrated by the Court's recent jurisprudence. Accordingly, the following section briefly considers cases in which technological developments have blurred this distinction, challenging the traditional boundaries of lawful surveillance.

The Blurred Line Between Mass and Targeted Surveillance

The rapid evolution of digital technologies is increasingly challenging the traditional dichotomy between targeted and mass surveillance. Encryption, anonymization tools, and the global flow of data have made conventional distinctions based on scope, selectivity or purpose increasingly blurred. In several recent cases, the ECtHR has confronted surveillance practices that, while formally targeted, relied on mass interception or algorithmic filtering of vast data sets to identify potential threats. Such techniques effectively merge preventive intelligence gathering with individualized monitoring, resulting in a hybrid form of surveillance.

Cases involving the surveillance of encrypted communications illustrate how the line between targeted and mass surveillance can quickly become blurred. They reveal broader structural challenges, including the fragmentation of procedural safeguards, the tension between investigative efficiency and the protection of fundamental rights, and the limitations of existing instruments such as the European Investigation Order (Turanjanin, 2025, p. 10). Investigations initially aimed at specific individuals or entities may ultimately affect thousands of users. One illustrative example is the EncroChat platform[8], where criminal proceedings against the company led to the interception of communications from thousands of users, subsequently triggering large-scale prosecutions (See more in: Bajović, 2022).

[8] EncroChat was an encrypted communication service primarily used via modified smartphones, marketed as a secure platform for private messaging. It was dismantled in a joint law enforcement operation in 2020, revealing widespread criminal use of the network (Europol, 2020).

The ECtHR addressed the surveillance of encrypted communications in *Yüksel Yalçınkaya v. Turkey [GC],* where the applicant's conviction was based on his use of the ByLock messaging app. Turkish authorities treated all users as members of the "Gülen movement," creating an almost irrebuttable presumption of guilt and denying individuals the chance to challenge the evidence. The Court found systemic violations of several Convention rights and ordered general measures on the judicial assessment of ByLock evidence (§§ 414, 416). However, it did not rule on the broader legality of encrypted communication surveillance (Škulić, 2024, pp. 38-39). The judgment illustrates the Court's cautious approach toward surveillance of encrypted communications, focusing on due process guarantees rather than on establishing broader principles governing state access to encrypted data.

When bulk interception tools are used to extract or analyse the communications of specific individuals, procedural safeguards designed for targeted surveillance must apply with equal rigor. Conversely, when targeted measures rely on large-scale data collection, states must ensure that prior judicial authorisation is obtained, that a procedurally relevant degree of suspicion exists linking a specific individual or group to criminal activity, that temporal limits are clearly defined, and that the necessity and proportionality of the measure are subject to continuous oversight throughout its implementation.

The Convention framework is designed to balance the imperatives of collective security with the protection of individual rights. However, the emergence of advanced surveillance technologies increasingly strains its capacity to preserve this equilibrium. Ensuring effective human rights protection therefore depends on the consistent application of Strasbourg standards of legality, independent oversight, data protection safeguards, proportionality and effective remedies to all emerging forms of surveillance, irrespective of their technical configuration.

Conclusion

The analysis demonstrates that, under the European Convention on Human Rights, mass surveillance of communications is permitted only conditionally and subject to a set of strict and cumulative Strasbourg standards developed in the jurisprudence of the European Court of Human Rights. Rather than rejecting bulk interception as such, the Strasbourg Court has articulated a framework within which its compatibility with the ECHR depends on the fulfillment of multiple interrelated standards, operationalised through corresponding safeguards.

Five core standards emerge consistently from the Court's case law: legality, independent oversight, data protection safeguards, proportionality, and effective remedies. These standards are cumulative rather than alternative; each loses meaning if not supported by the others. Legality structures the exercise of surveillance powers within a clear, accessible, and foreseeable legal framework. Independent oversight constrains executive discretion through mechanisms of authorization, supervision, and review. Data protection safeguards limit the collection, use, retention, and dissemination of intercepted data. Proportionality requires

that all measures remain necessary and strictly limited to the legitimate aim pursued. Finally, effective remedies ensure that surveillance measures are subject to mechanisms of institutional review and accountability capable of identifying, correcting, and, where appropriate, redressing unlawful interferences, even in the absence of individual notification.

Taken together, these standards, reflected through a set of cumulative safeguards, constitute a systematic model of human rights compliance under the Convention. Their interdependence implies that weaknesses in one dimension (e.g. oversight) cannot be compensated by the formal strength of another (e.g. legality). Strasbourg case law thus offers not only a catalogue of standards but a functional framework for assessing whether national surveillance regimes respect the essence of the right to privacy.

The findings further indicate that compliance with Strasbourg standards depends not only on their formal recognition in domestic law, but also on their effective implementation in practice. The operation of independent supervisory bodies, the quality of judicial review, and the institutional capacity to enforce data protection requirements play a decisive role in determining whether surveillance frameworks function in a Convention-compliant manner. In this respect, the Court's case law highlights structural risks that may arise where safeguards remain declarative rather than operational. At the international level, the lack of harmonized rules governing cross-border access to and exchange of intercepted data presents additional challenges for the effective application of Convention standards. Differences between national legal regimes may create gaps in oversight and accountability, particularly in relation to metadata processing and international intelligence cooperation.

Overall, Strasbourg case law offers a structured set of safeguards for assessing mass surveillance under the Convention, which form cumulative standards according to which such measures can be considered compatible with the rights and freedoms protected by the Convention.

References

Bajović, V. (2022) 'EncroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku', *CRIMEN*, *13*(2), 154-179. https://doi.org/10.5937/crimen2202154B

Barocas, S. and Selbst, A.D. (2016) 'Big data's disparate impact', *Calif. L. Rev.*, 104, 671-732. https://doi.org/10.2139/ssrn.2477899

Bernal, P. (2016) 'Data gathering, surveillance and human rights: recasting and debate', *Journal of Cyber Policy*, *1*(2), 243-264. https://doi.org/10.1080/23738871.2016.1228990

Bernal, P. (2018) *The Internet, warts and all: Free speech, privacy and truth*. Cambridge: Cambridge University Press.

Beširević, V. *et al*. (2017) *Komentar Konvencije za zaštitu ljudskih prava i osnovnih sloboda*. Beograd: Službeni glasnik.

Carpenter, C. (2020) 'Privacy and proportionality: Examining mass electronic surveillance under Article 8 and the Fourth Amendment', *International and Comparative Law Review*, *20*(1), 27-57. https://doi.org/10.2478/iclr-2020-0002

Celeste E. and Formici G. (2024) 'Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia', *German Law Journal*, *25*(3), 427-446. https://doi.org/10.1017/glj.2023.105

Dajović, G. and Spaić, B. (2019) 'Doktrina "četvrte instance" i pravo na obrazloženu presudu u praksi Evropskog suda za ljudska prava', *Anali Pravnog fakulteta u Beogradu*, *67*(3), 158-185. https://doi.org/10.5937/AnaliPFB1903166D

ECtHR, *Airey v. Ireland*, no. 6289/73, Judgment of 9 October 1979 (*Airey v. Ireland*)

ECtHR, *Big Brother Watch and Others v. UK*, nos. *58170/13, 62322/14 and 24960/15*, Judgment of 25 May 2021[GC] (*Big Brother Watch and Others v. UK* [GC])

ECtHR, *Centrum för rättvisa v. Sweden*, no. 35252/08, Judgment of 25 May 2021 [GC] (*Centrum för rättvisa v. Sweden* [GC])

ECtHR, *Copland v. UK*, no. 62617/00, Judgment of 03 April 2007 (*Copland v. UK*)

ECtHR, *Djavit An v. Turkey*, no. 20652/92, Judgment of 20 February 2003 (*Djavit An v. Turkey*)

ECtHR, *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022 (*Ekimdzhiev and Others v. Bulgaria*)

ECtHR, *Glukhin v. Russia*, no. 11519/20, Judgment of 4 July 2023 (*Glukhin v. Russia*)

ECtHR, *Gorzelik and Others v. Poland*, no. 44158/98, Judgment of 17 February 2004 (*Gorzelik and Others v. Poland*)

ECtHR, *Guja v. Moldova* [GC], no. 14277/04, Judgment of 12 February 2008 [GC] (*Guja v. Moldova* [GC])

ECtHR, *Huhtamäki v. Finland*, no. 54468/09, Judgment of 6 March 2012 (*Huhtamäki v. Finland*)

ECtHR, *Iordachi and Others v. Moldova*, no. 25198/02, Judgment of 10 February 2009 (*Iordachi and Others v. Moldova*)

ECtHR, *Iovchev v. Bulgaria*, no. 41211/98, Judgment of 2 February 2006 (*Iovchev v. Bulgaria*)

ECtHR, *Jalloh v. Germany*, no. 54810/00, Judgment of 11 July 2006 [GC] (*Jalloh v. Germany* [GC])

ECtHR, *Kafkaris v. Cyprus*, no. 21906/04, Judgment of 12 February 2008 [GC] (*Kafkaris v. Cyprus* [GC])

ECtHR, *Kennedy v. UK*, no. 26839/05, Judgment of 18 May 2010 (*Kennedy v. UK*)

ECtHR, *Kononov v. Latvia*, no. 36376/04, Judgment of 17 May 2010 [GC] (*Kononov v. Latvia* [GC])

ECtHR, *Leander v. Sweden*, no. 9248/81, Judgment of 26 March 1987 (*Leander v. Sweden*)

ECtHR, *Lorse and Others v. Netheralands*, no. 52750/99, Judgment of 4 February 2003 (*Lorse and Others v. Netheralands*)

ECtHR, *Malone v. UK*, no. 8691/79, Judgment of 2 August 1984 (*Malone v. UK*)

ECtHR, *Marinković v. Serbia*, no. 5353/11, Judgment of 22 October 2013 (*Marinković v. Serbia*)

ECtHR, *Michaud v. France*, no. 12323/11, Judgment of 6 December 2012 (*Michaud v. France*)

ECtHR, *Miroļubovs and Others v. Latvia*, no. 798/05, Judgment of 15 September 2009 (*Miroļubovs and Others v. Latvia*)

ECtHR, *Okpisz v. Germany,* no. 59140/00, Judgment of 25 October 2005 (*Okpisz v. Germany*)

ECtHR, *Pietrzak and BychawskaSiniarska and Others v. Poland,* nos. 72038/17 and 25237/18 Judgment in French of 3 February 2022 (*Pietrzak and BychawskaSiniarska and Others v. Poland*)

ECtHR, *Podchasov v. Russia*, no. 33696/19, Judgment of 13 February 2024 (*Podchasov v. Russia*)

ECtHR, *Roman Zakharov v. Russia*, no. 47143/06, Judgment of 4 December 2015 [GC] (*Roman Zakharov v. Russia* [GC])

ECtHR, *Rotaru v. Romania*, no. 28341/95, Judgment of 4 May 2000 (*Rotaru v. Romania*)

ECtHR, *Segerstedt-Wiberg and Others v. Sweden,* no. 62332/00, Judgment of 6 June 2006 (*Segerstedt-Wiberg and Others v. Sweden*)

ECtHR, *Sunday Times v. UK*, no. 6538/74, Judgment of 26 April 1979 (*Sunday Times v. UK*)

ECtHR, *Weber and Saravia v. Germany*, no. 54934/00, Judgment of 29 June 2006 (*Weber and Saravia v. Germany*)

ECtHR, *Yüksel Yalçınkaya v. Turkey*, no. 15669/20, Judgment of 26 September 2023 [GC] *(Yüksel Yalçınkaya v. Turkey* [GC])

Europol (2020) *Dismantling of encrypted network sends shockwaves through organised crime groups across Europe*. Available at: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe(Accessed: 15 September 2025)

Ilić, G. P. (2011) 'Pravo na obrazloženu sudsku odluku', *CRIMEN*, *2*(2), 227-244.

Ilić, G. P. (2015) 'O nezakonitim dokazima u krivičnom postupku', *Kaznena reakcija u Srbiji*, 5, 75-87.

Ilić, G. P. (2021) 'Arbitrarna primena prava i pravo na pravično suđenje', *Kaznena reakcija u Srbiji*, 11, 120-138.

Joint Committee on the Draft Investigatory Powers Bill (2016) *Oral Evidence: Draft Investigatory Powers Committee*. Available at: https://www.parliament.uk/globalassets/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf (Accessed: 17 September 2025)

Kosta, E. (2020) 'Algorithmic state surveillance: Challenging the notion of agency in human rights', *Regulation & Governance,* 16, 212-224. https://doi.org/10.1111/rego.12331

Logan, S. (2017) 'The needle and the damage done: Of haystacks and anxious panopticons', *Big Data & Society*, *4*(2), 1-13. https://doi.org/10.1177/20539517177345

Lynskey, O. (2023) 'Complete and effective data protection', *Current Legal Problems*, *76*(1), 297-343. https://doi.org/10.1093/clp/cuad009

Macnish, K. (2020) 'Mass surveillance: A private affair?', *Moral Philosophy and Politics*, *7*(1), 9-27. https://doi.org/10.1515/mopp-2019-0025

Miljuš I. (2021) *Načelo jednakosti "oružja" u krivičnom postupku*. Doktorska disertacija. Univerzitet u Beogradu.

Mitsilegas, V. *et al*. (2023) 'Data retention and the future of large scale surveillance: The evolution and contestation of judicial benchmarks', *European Law Journal*, *29*(1-2), 176-211. https://doi.org/10.1111/eulj.12417

Murray, D. and Fussey, P. (2019) 'Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data', *Israel Law Review*, *52*(1), 31-60. https://doi.org/10.1017/s0021223718000304

Newell, B. C. (2014) 'The massive metadata machine: Liberty, power, and secret mass surveillance in the US and Europe', *ISJLP*, *10*(2), 481-522.

Nissenbaum, H. (2010) *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Paunović, M. and Carić, S. (2006) *Evropski sud za ljudska prava osnovna načela i tok postupka*. Beograd: Pravni fakultet Univerziteta u Beogradu.

Pisarić, M. (2022) 'Communications encryption as an investigative obstacle', *Revija za kriminologiju i krivično pravo*, *60*(1), 61-74. https://doi.org/10.47152/rkkp.60.1.4

Popović, D. (2008) *Evropski sud za ljudska prava: između 11. i 14. dodatnog protokola uz konvenciju za zaštitu ljudskih prava i osnovnih sloboda*. Beograd: Službeni glasnik.

Popovic, D. (2011) 'Uticaj Evropske Konvencije za zaštitu ljudskih prava i osnovnih sloboda na srpsko zakonodavstvo i sudsku praksu', *Pravni Zapisi*, *2*(2), 343-357. https://doi.org/10.5937/pravzap1102343p

Richards, J. (2019) 'Needles in haystacks: law, capability, ethics, and proportionality in big data intelligence-gathering', *Secret Intelligence*, 2, 422-431. https://doi.org/10.4324/9780429029028-28

Rojszczak, M. (2021) 'Extraterritorial bulk surveillance after the German BND act judgment', *European Constitutional Law Review*, *17*(1), 53-77. https://doi.org/10.1017/S1574019621000055

Škulić, M. (2024) 'Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje - kao što su Sky ecc i Enchrochat', *CRIMEN*, *15*(1), 3-55. https://doi.org/10.5937/crimen2401003S

Slobogin, C. (2015) 'Standing and covert surveillance', *Pepperdine Law Review*, *42*(3), 517-548.

Snowden, J. (2014) *Snowden Answers Our Burning Data Collection Question: What's the Worst That Could Happen?* Available at: https://techcrunch.com/2014/01/23/snowden-answers-our-burning-data-collection-question-whats-the-worst-that-could-happen/ (Accessed: 01 September 2025)

Turanjanin, V. (2025) 'EncroChat, Sky ECC and Regulation (EU) 2023/1543: towards a new standards of digital evidence (I)', *Revija za kriminologiju i krivično pravo*, 62(1), 7-30. https://doi.org/10.47152/rkkp.63.3.1

Van der Sloot, B. (2020) 'The quality of law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 11, 160-185.

Vogiatzoglou, P. (2019) 'Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity', *European Journal of Law and Technology*, *10*(1).

Watt, E. (2017) 'The right to privacy and the future of mass surveillance', *The International Journal of Human Rights*, *21*(7), 773–799. https://doi.org/10.1080/13642987.2017.1298091

Xu, X. (2021) 'To repress or to co-opt? Authoritarian control in the age of digital surveillance', *American Journal of Political Science*, *65*(2), 309-325. https://doi.org/10.1111/ajps.12514

Zalnieriute, M. (2022) 'Big brother watch and others v. the United Kingdom', *American Journal of International Law*, *116*(3), 585-592. https://doi.org/10.1017/ajil.2022.35