International Journal of Law and Societal Studies
ISSN: 3079-2614
DOI: 10.61424/ijlss
Journal Homepage: www.bluemarkpublishers.com/index.php/IJLSS

IJLSS
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Balancing Security and Privacy: Analyzing the Effectiveness of EU Digital Surveillance Laws in Criminal Proceedings

Shpëtim KARAKUSHI PhD
Faculty of Economics, Law and Social Sciences, University College of Business, Tirana, Albania
Corresponding Author: Shpëtim KARAKUSHI PhD, **E-mail**: shpetimkarakushi@gmail.com

| ABSTRACT
This research examines the complex balance between privacy and law enforcement in EU digital surveillance laws during criminal proceedings. It analyzes how these laws protect individual rights while ensuring security through case studies and legal analysis. Landmark cases like Digital Rights Ireland, Schrems decisions, and Tele2 Sverige illustrate the European courts' preference for targeted surveillance over mass data collection, highlighting tensions between privacy and security. Although these laws provide essential privacy safeguards, challenges exist in their practical application, especially in cross-border investigations. The study concludes with suggestions to improve the efficacy of these laws, ensuring they uphold fundamental rights protections effectively.

| KEYWORDS
Digital surveillance, EU law, privacy rights, criminal proceedings, data retention, GDPR, case law analysis.

| ARTICLE INFORMATION
ACCEPTED: 01 August 2025 **PUBLISHED:** 26 September 2025 **DOI:** 10.61424/ijlss.v2.i1.445

1. Introduction

Every digital activity, like phone calls, website visits, and messages, leaves a trace that can be stored and analyzed. In Europe, citizens benefit from unique protections due to years of legal battles, court decisions, and laws aimed at balancing security and privacy in the digital world.

The European Union has positioned itself as a global leader in digital rights protection, yet it simultaneously faces mounting pressure to provide law enforcement agencies with the tools they need to combat increasingly sophisticated criminal activities [1]. The core issue in EU digital surveillance law is balancing individual privacy with collective security, affecting over 450 million European citizens. These laws are not just abstract concepts but influence everyday activities like sending encrypted messages, processing data, and investigating cybercrimes. The evolution of these laws involves legal advancements, political negotiations, and judicial rulings. The story of EU digital surveillance is about making choices regarding societal values, risks, and the balance between freedom and security. Initially, the focus was on adapting traditional law enforcement methods for the digital age, but concerns about the potential overreach of surveillance powers have arisen. The research paper investigates legal texts, landmark cases, and current frameworks to evaluate and improve the effectiveness of handling cybercrimes. The EU's approach to balancing security and privacy in digital rights is influential globally, affecting discussions in other regions facing similar challenges. Understanding how well this model works—where it succeeds, where it falls short, and how it might be improved—has implications that reach far beyond Europe's borders. This research will take through the complex web of EU legislation, from the now-invalidated Data Retention Directive to the comprehensive framework of the General Data Protection Regulation (GDPR), from the emerging Digital Services

Act to the specialized rules governing electronic evidence in criminal proceedings. But more than just examining these laws on paper, we'll look at how they've been interpreted and applied by courts, how they've been implemented by member states, and how they've affected real criminal investigations. This research uses a blend of traditional legal analysis and case studies, considering court decisions, legislative documents, and academic insights from the EU. This method helps explore the practical workings of laws in criminal investigations and digital rights protection. It acknowledges that EU digital surveillance law is continually evolving. New technologies constantly challenge existing legal frameworks, new threats emerge that test the adequacy of current protections, and new court decisions continue to refine and reshape the legal landscape. This research also examines how to balance surveillance and privacy in democratic societies. It highlights that inadequate surveillance can hamper law enforcement and national security, while excessive surveillance can threaten democratic values and individual freedoms. The study analyzes legal frameworks and their practical applications to help guide discussions on maintaining security without compromising privacy rights. This understanding is vital for addressing current legal and policy issues, ensuring that privacy rights fundamental to human dignity and democratic governance are upheld.

2. Literature Review and Legal Framework Analysis

2.1 The Evolution of Digital Surveillance Discourse

The evolution of EU digital surveillance laws over the past 20 years highlights significant changes due to advancing technologies and improving legal strategies. Initial academic work mainly reacted to new technologies, lacking a full understanding of their long-term impact on law and privacy[2]. Privacy scholars have identified the insufficiency of traditional legal systems to tackle digital surveillance. Key researchers, like Tuomas Ojanen, analyzed electronic surveillance in light of important cases, showing how European courts uniquely balance surveillance powers with the protection of fundamental rights [3]. What makes the European approach particularly fascinating from an academic perspective is its emphasis on proportionality and necessity as core principles governing surveillance activities. Unlike other jurisdictions that have adopted more permissive approaches to digital surveillance, EU law has consistently required that surveillance measures be both necessary for achieving legitimate aims and proportionate to the threats they address. The principle-based approach has resulted in a substantial amount of case law affecting global discussions on surveillance governance. Scholars' views on digital surveillance have shifted, moving from believing more surveillance equals better security to questioning its effectiveness. An EU-funded study by SURVEILLE highlights electronic mass surveillance's failure in meeting security goals, prompting a reevaluation of its cost-benefit analysis[4]. This finding is particularly significant because it challenges one of the core justifications for expansive surveillance powers, that they are necessary for effective law enforcement and national security. The SURVEILLE study's conclusion that mass surveillance is not only ineffective but may actually be counterproductive has influenced subsequent policy discussions and court decisions across the EU.

2.2 The Legal Architecture of EU Digital Surveillance

The EU's digital surveillance laws are complex, with multiple regulations that can be unpredictable. The EU Charter of Fundamental Rights is key, particularly Articles 7 and 8, which focus on respecting private and family life and protecting personal data[5-6]. The General Data Protection Regulation (GDPR) represents perhaps the most comprehensive attempt by any jurisdiction to regulate the processing of personal data, including data used for surveillance purposes. However, the GDPR's relationship with law enforcement activities is complicated by the existence of specific exemptions and the parallel Law Enforcement Directive, which governs data processing by competent authorities for criminal law enforcement purposes [7]. The regulatory landscape aims to balance strong privacy protections with the needs of law enforcement. However, unclear boundaries between different regulations create uncertainty for law enforcement agencies and service providers. The ePrivacy Directive adds complexity by focusing on communication confidentiality and traffic data processing, asserting that traffic data should be deleted or anonymized when no longer needed. Recent EU legislation, including the Digital Services Act, further imposes new obligations on online platforms to cooperate with law enforcement while ensuring the protection of users' fundamental rights. The proposed e-Evidence Regulation aims to streamline cross-border access to electronic evidence while maintaining appropriate safeguards for privacy and data protection [8].

2.3 Theoretical Frameworks for Understanding Surveillance Governance

Academic analysis of EU digital surveillance laws has been enriched by the application of various theoretical frameworks that help explain both the development and effectiveness of these legal tools. The most known of these is the *proportionality principle*, which has become central to European approaches to surveillance governance. Proportionality, as applied in the EU context, requires that surveillance measures be suitable for achieving their stated objectives, necessary in the sense that no less intrusive measures would be equally effective, and proportionate in the narrow sense that the benefits achieved justify the interference with fundamental rights[9]. The EU uses a three-part test to evaluate surveillance measures, but its real-world application is more complicated than it seems. The "*essence*" concept is also key, as the Court of Justice states some surveillance measures violate fundamental rights' essence, making them unacceptable despite safeguards[10]. This concept has proven to be particularly significant in cases involving mass surveillance, where the court has found that the indiscriminate collection of personal data may violate the essence of privacy rights even when subject to subsequent limitations on access and use [11]. Another important theoretical framework is the notion of "*surveillance capitalism*," developed by Shoshana Zuboff, which helps explain how commercial surveillance practices intersect with law enforcement surveillance [12]. This framework has become increasingly relevant as EU lawmakers with the role of private companies in surveillance systems and the extent to which commercial data collection practices should be regulated to prevent their exploitation for surveillance purposes. The literature also reveals growing attention to the concept of "*privacy by design*" and "*data protection by design*," which require that privacy and data protection considerations be integrated into surveillance systems from their inception rather than added as an afterthought[13]. Technical design choices impact privacy, independent of the governing legal framework.

2.4 Empirical Research on Surveillance Effectiveness

Recent research highlights the growing empirical research on digital surveillance's effectiveness, challenging assumptions about its link to security. This research shows a complex reality often overlooked by policymakers. A key issue is the lack of reliable data, as governments are hesitant to provide details on surveillance programs, complicating thorough empirical evaluation of their effectiveness [14]. Data scarcity impacts policy discussions on surveillance powers, as decisions are often made without solid evidence. Available data shows that data retention programs generate lots of data but may not improve law enforcement outcomes compared to targeted methods [15]. This calls into question their necessity under EU surveillance law. Research on cross-border criminal investigations highlights challenges in implementing EU legislation due to differences in legal systems, technical capabilities, and cultures, indicating that legal harmonization alone are insufficient.

2.5 The Role of Technology in Shaping Legal Frameworks

The relationship between technology and law in surveillance is complex. New technologies often outpace legal frameworks, creating gaps that need legislative attention. Conversely, laws influence the design of technology, requiring compliance with privacy protection[16]. Artificial intelligence plays a key role, offering data analysis capabilities but also raising new privacy concerns. The EU's proposed AI Act addresses these issues, yet AI and surveillance law continue to evolve. Encryption technologies present another set of challenges for surveillance law. While encryption is essential for protecting privacy and security in digital communications, it can also limit law enforcement's ability to access communications content even when legally authorized to do so. The EU has generally taken a more privacy-protective approach to encryption than some other jurisdictions, but tensions remain between privacy advocates who want strong encryption protections and law enforcement agencies who seek access capabilities. New communication platforms like messaging apps complicate traditional surveillance regulation due to their cross-border nature. The EU's eEvidence Regulation tries to manage these challenges while protecting privacy [17].

2.6 Comparative Perspectives and Global Influence

The EU's approach to digital surveillance law has not developed in isolation but has been influenced by developments in other jurisdictions. Comparative analysis reveals that the EU has generally adopted a more privacy-protective approach than countries like the United States or China, but it has also been more willing to regulate surveillance activities than some other democratic jurisdictions[18]. The EU's surveillance laws, particularly the GDPR,

have had a significant global impact, influencing privacy regulations in many countries. This "*Brussels Effect*" is notable in data protection, but less so in surveillance laws due to national sovereignty and security concerns. Academic studies highlight the strengths and limitations of the EU approach, noting that varying implementation and enforcement across member states affect its overall effectiveness and suggest the need for better coordination [19].

The literature also reveals ongoing tensions between different models of surveillance governance. The EU's emphasis on proportionality and fundamental rights protection contrasts sharply with approaches in other jurisdictions that prioritize security concerns or economic interests [20-21]. Understanding EU laws' global context highlights unique strengths and challenges as different philosophical views on the individual-state relationship affect international discourse on surveillance.

3. Case Study Analysis: Landmark Decisions Shaping EU Digital Surveillance Law

3.1 The Digital Rights Ireland Revolution: Striking Down Mass Surveillance

Digital Rights Ireland, led by TJ McIntyre, challenged extensive EU digital surveillance programs. Their seven-year legal battle significantly changed European court perspectives on mass surveillance and data retention, influencing modern EU digital surveillance laws[3]. The case centered on the EU Data Retention Directive (2006/24/EC), which required telecommunications providers across the EU to retain traffic and location data for all communications for periods ranging from six months to two years[22]. The directive was designed as a response to digital security challenges, with law enforcement needing access to metadata to investigate serious crimes and prevent terrorism. It was supported politically and adopted by EU member states. However, Digital Rights Ireland [23] opposed it, viewing the directive as a comprehensive surveillance system that recorded every individual's communication patterns, regardless of any wrongdoing. This included phone calls, text messages, emails, and website visits, all accessible to law enforcement. The legal challenge by Digital Rights Ireland was based on the belief that the directive violated privacy and data protection rights outlined in the EU Charter of Fundamental Rights. They argued mass data retention conflicted with the principles of necessity and proportionality. The Court of Justice of the European Union was asked in this case, if the Data Retention Directive was compatible with the EU Charter of Fundamental Rights, and what principles should guide data retention for law enforcement. In April 2014, the CJEU unanimously invalidated the Data Retention Directive, citing violations of privacy and data protection rights[24]. The court made a decisive ruling that has influenced EU surveillance law by establishing key principles. It declared that the broad, indiscriminate retention of electronic communication data for everyone was disproportionate and violated fundamental rights. This directive, without differentiating or providing exceptions for combating serious crimes, impacted almost the entire European population, leading to unprecedented privacy interference. The court highlighted major issues with the directive, noting the absence of proper safeguards for data access, which were not limited to necessary instances or subject to review by a court or authority. Additionally, the directive lacked adequate data security measures and provisions to keep data within the EU's protection standards. The Digital Rights Ireland decision had a significant impact on mass data retention practices across the EU. Member states reassessed their laws, with some suspending programs and others seeking new, compliant methods. This ruling also affected law enforcement, which relied on retained data for criminal investigations. Importantly, the decision established that mass surveillance violates EU fundamental rights, regardless of data access safeguards. This principle favored targeted surveillance, influenced court decisions and legislation, and demonstrated how civil society can challenge surveillance through legal action.

3.2 The Schrems Saga: Transatlantic Data Flows and Surveillance Oversight

While Digital Rights Ireland focused on surveillance within the EU, the series of cases brought by Austrian privacy activist Max Schrems addressed the equally complex question of how EU privacy rights apply when personal data is transferred to third countries with different surveillance regimes[3]. The Schrems cases concern the conflict between European privacy standards and American surveillance practices. It began when Max Schrems filed a complaint in 2013 against Facebook Ireland, arguing that transferring his data to the US violated EU privacy laws, especially after Edward Snowden revealed NSA surveillance. Schrems claimed the US Safe Harbor framework did not protect against this surveillance. In 2015, the Court of Justice of the European Union invalidated Safe Harbor,

causing disruption in data transfers and leading to a new agreement, the Privacy Shield. Schrems challenged this in 2017 in the Schrems II case, arguing it still didn't align US surveillance with EU privacy rights.

The Schrems II decision, delivered by the CJEU in July 2020, was even more far-reaching than its predecessor. The court invalidated the Privacy Shield adequacy decision, finding that US surveillance laws still did not provide adequate protection for EU personal data [25]. The court was particularly critical of Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, which it found allowed for mass surveillance that was incompatible with EU fundamental rights. The court raised concerns about using Standard Contractual Clauses for data transfers to countries with significant surveillance powers, requiring case-by-case assessments to ensure data protection. The Schrems II decision has significantly impacted businesses, causing many to move data processing to the EU or use additional technical measures like encryption. This decision has influenced data transfer practices globally, as companies now assess surveillance risks in other countries as well [26]. The Schrems cases clarified EU surveillance law, confirming that EU privacy rights apply to surveillance by non-EU governments, economic factors cannot override fundamental rights, and safeguards must be practically effective. The Schrems cases highlight the complexity of surveillance laws in a globalized world with cross-border data flows. They compelled European policymakers to address the issue of safeguarding EU citizens' privacy by limiting not only EU but also third-country access to personal data.

3.3 Tele2 Sverige: Refining the Boundaries of Acceptable Surveillance

The Tele2 Sverige case, decided by the CJEU in December 2016, represented the court's first major opportunity to clarify and refine the principles established in Digital Rights Ireland. The case arose from challenges to national data retention laws in Sweden and the United Kingdom, providing the court with an opportunity to address some of the practical questions left unanswered by the earlier decision [27]. The Swedish case involved Tele2 Sverige challenging Sweden's data retention laws after the EU Data Retention Directive was invalidated, with Sweden arguing its laws were more compliant with EU law. In the UK, a similar challenge occurred with the Data Retention and Investigatory Powers Act 2014. These cases questioned the application of EU principles from Digital Rights Ireland to data retention, exploring if general retention by member states is possible with safeguards, what safeguards are necessary, and their relevance to national security. The court clarified and restricted by affirming that Digital Rights Ireland principles apply to all general data retention schemes, regardless of their legal basis. The court found that general and indiscriminate retention of traffic and location data was incompatible with EU law, even when accompanied by safeguards governing access to retained data [28]. The ruling blocked a path that many EU member states hoped to use to continue their data retention programs by rejecting the general and indiscriminate data collection due to its violation of fundamental rights. However, it didn't completely ban data retention, allowing it under strict conditions in serious crime investigations with limitations and independent reviews. Member states must ensure their national security activities respect EU fundamental rights. This controversial decision, known as the Tele2 Sverige case, led to immediate changes in several member states' programs and affected EU legislative discussions, with the European Commission deciding not to propose a new directive. It highlighted the ongoing conflict between fundamental rights and law enforcement needs, strengthening Digital Rights Ireland principles and impacting future cases and legislation.

3.4 The Prokuratuur Case: Independence and Proportionality in Data Access

The 2021 Prokuratuur case provided the CJEU with an opportunity to further refine the principles governing access to retained communications data, focusing particularly on the requirement for independent oversight of surveillance activities [29]. The case arose from a reference by the Estonian Supreme Court regarding the compatibility of Estonian law with EU requirements for independent authorization of access to traffic and location data. Prosecutors in Estonia could approve access to communications data without court approval. The government claimed they were impartial, but the CJEU ruled they are too involved in investigations, stressing the need for an independent authority for data access oversight [30]. The Prokuratuur case established the need for independent judicial or similar authorization to access communications data, especially in serious crime cases. The decision emphasized the importance of protecting fundamental rights, not only through procedural rules but also by ensuring independent oversight of surveillance activities. It addressed the scope and purpose of accessing such

data, specifying that it must be strictly necessary for investigating serious crimes and consider proportionality, balancing the crime's severity against the surveillance's intrusiveness. This ruling impacted several member states with legal systems allowing non-judicial authorities to authorize data access, prompting them to revise their procedures to meet these oversight requirements. The case highlighted the CJEU's dedication to setting specific, practical guidelines for surveillance oversight, beyond general principles, aligning with EU fundamental rights.

3.5 Comparative Analysis: Patterns and Principles Across Cases

The Court of Justice of the European Union (CJEU) prioritizes fundamental rights over security and economic concerns in digital surveillance law. This reflects a European perspective that favors individual rights over state power. The CJEU prefers targeted surveillance rather than mass surveillance, finding general surveillance incompatible with EU rights, regardless of safeguards. It requires independent oversight, insisting on judicial or independent authorization for effective rights protection. The court applies EU privacy rights broadly, affecting both EU and non-EU surveillance involving EU data. Decisions like invalidating the Data Retention Directive and Privacy Shield highlight its focus on rights but pose challenges in balancing security and legal compliance. Privacy advocates praise the approach for protecting rights, while law enforcement finds it complicates security efforts. These principles continue to shape EU and global surveillance law and policy.

4. Methodology

The research used a mixed approach, combining legal analysis and real-world case studies, to assess how well EU digital surveillance laws work in criminal cases. The aim was to understand both the legal framework and its application in real situations. The legal analysis involved studying EU treaties, regulations, directives, and important court decisions, with a focus on key cases from the Court of Justice of the European Union (CJEU) that shape the interpretation and application of the laws. Academic commentary, policy documents, and other studies were also reviewed for additional context. The case studies examined three areas: key court decisions that define surveillance limits, challenges for member states in implementing EU laws nationally, and examples of cross-border cooperation involving electronic evidence in investigations. This approach looked at both the theoretical soundness and practical effectiveness of EU surveillance laws. Data was collected from court decisions, legislative documents, academic literature, and policy reports, but detailed operational data was scarce due to the sensitivity and secrecy of surveillance activities. The analysis employed both qualitative and quantitative methods where appropriate, though the predominantly legal nature of the research meant that qualitative analysis was the primary analytical approach. The research was conducted with attention to the evolving nature of the field, recognizing that digital surveillance law continues to develop rapidly in response to technological changes and new security challenges.

5. Results and Discussion

5.1 Qualitative Results: Strengthening Rights while Constraining Capabilities

The analysis of EU digital surveillance laws highlights a significant paradox in current governance. On one hand, these laws have strengthened privacy protections and set important limits on surveillance, as seen in court cases where EU courts have struck down major surveillance programs failing to protect fundamental rights. This approach has real-world effects, such as the overturning of the Data Retention Directive, prompting member states to adopt more focused surveillance tactics. The Schrems rulings have also reshaped the global data economy by pushing companies towards better privacy practices and restricting non-EU governments' access to European personal data. However, these increased privacy protections have impacted law enforcement capabilities. Authorities argue that the restrictions make it harder to investigate crimes, especially in cases of terrorism, organized crime, and cybercrime. The absence of broad data retention is seen as a major obstacle to such investigations. Evaluating the trade-off between privacy and security is challenging since privacy is subjective and security benefits are hard to assess independently. Consequently, this difficulty in measurement leads to ongoing debates about finding the right balance between ensuring security and protecting privacy.

What the research does reveal is that the EU's approach to surveillance governance reflects a distinctive set of values and priorities that differ significantly from those of other major jurisdictions. The consistent prioritization of

fundamental rights over security considerations, even when the security stakes are high, reflects a European commitment to constitutional democracy and the rule of law that has deep historical roots.

5.2 Implementation Challenges: From Legal Principles to Operational Reality

The research highlights a significant gap between EU surveillance law principles and their practical implementation by member states. While the Court of Justice of the EU (CJEU) has set clear rules for surveillance, applying them in real-world systems is difficult. One challenge is the technical complexity of modern surveillance systems. The court's requirement for targeted, not mass, surveillance needs advanced technology to focus only on necessary data for investigations. However, many law enforcement agencies lack the necessary technical skills and resources. Another issue is the need for independent oversight of surveillance activities, often requiring new institutional arrangements, which can be politically and administratively difficult. Additionally, the cross-border nature of investigations poses challenges, as EU law relies on frameworks for sharing electronic evidence, but practical cooperation often depends on informal relationships and technical compatibility between national systems. These practical factors can significantly affect the effectiveness of EU surveillance law in addressing cross-border crimes. The research also reveals significant variation in how member states have implemented EU surveillance requirements. Some countries have embraced the court's privacy-protective approach and have developed innovative solutions that provide strong privacy protections while still enabling effective law enforcement. Others have been more resistant to change and have implemented only the minimum requirements necessary to comply with EU law. This variation in implementation approaches has important implications for the overall effectiveness of EU surveillance law. In areas where implementation is inconsistent or incomplete, the privacy protections established by EU law may be undermined, and the effectiveness of cross-border cooperation may be reduced. This suggests that ongoing monitoring and enforcement of implementation requirements may be necessary to ensure that EU surveillance law achieves its intended objectives.

5.3 The Global Dimension: EU Law in an Interconnected World

The Schrems I and II cases highlight the global nature of surveillance governance and the challenges posed to regional privacy protection efforts. In a world interconnected by data crossing borders and involving multiple jurisdictions, the effectiveness of EU surveillance law relies not only on internal EU actions but also on its interaction with other countries' surveillance regulations. To tackle this, the EU has extended its privacy protections' reach beyond its borders, applying fundamental EU rights to surveillance involving EU personal data, even by third countries. This approach, however, has sparked controversy and tension, particularly with the United States, due to differing surveillance governance methods. This extraterritorial strategy has seen mixed results. It has prompted some adjustments in third-country surveillance practices and strengthened international data transfer agreements' privacy protections. For example, the Privacy Shield framework, although later invalidated, included U. S. commitments to limit surveillance activities. However, the approach also presents challenges for international law enforcement cooperation and has led to the fragmented global data economy. Some countries responded with data localization demands or reduced cooperation with EU agencies. With other major regions developing their own surveillance systems, the EU may struggle to sustain its privacy-focused approach without hampering international collaboration or addressing global security challenges

5.4 Technological Evolution and Legal Adaptation

The fast development of technology challenges EU surveillance law and questions how well the legal framework can adapt, especially with technologies like AI, quantum computing, and advanced encryption. These advancements provide new surveillance abilities but also pose privacy risks. The EU is working on new laws, such as the AI Act and revised ePrivacy Regulation, to deal with these issues. However, laws often evolve slower than technology, leading to uncertainty about how existing laws apply. Research indicates that EU courts will likely use existing fundamental rights principles for new technologies, but how this works in practice remains unclear. The belief that mass surveillance conflicts with EU fundamental rights might need reevaluation due to AI's ability to analyze data without human input. Additionally, technical design choices greatly affect the privacy impact of surveillance systems, emphasizing the need for systems designed with privacy from the start.

5.5 Measuring Effectiveness

Evaluating the effectiveness of EU digital surveillance laws requires using different criteria due to varying perspectives among stakeholders. From a rights-protection perspective, EU surveillance laws are deemed successful, offering strong privacy and data protection rights, with courts upholding these even over security or economic interests. This has influenced global privacy standards by promoting international privacy values. However, its impact on law enforcement is mixed, as it requires more focused surveillance methods, potentially complicating efforts and hindering crime prevention for some officials. From a governance standpoint, EU laws effectively restrict surveillance power, ensuring oversight and emphasizing the necessity to prevent abuse. The research suggests that evaluating EU surveillance law effectiveness should include multiple criteria, considering both immediate and long-term impacts on democratic governance, international cooperation, and technological development.

6. Conclusions and Recommendations

The analysis of EU digital surveillance laws highlights a legal framework that effectively protects privacy but faces challenges in balancing these protections with security needs. The European model emphasizes strong rights protections, judicial oversight, and targeted rather than mass surveillance, influencing global policy debates. Significant achievements include landmark cases setting legal principles, the invalidation of programs like the Data Retention Directive, and extending EU privacy rights beyond borders, impacting international surveillance governance discussions. However, the research also reveals significant limitations and challenges. The implementation of EU surveillance law has been uneven across member states, creating gaps in protection and obstacles to effective cross-border cooperation. The restrictions on surveillance capabilities have created genuine challenges for law enforcement agencies, particularly in addressing sophisticated criminal organizations and emerging security threats. The rapid advancement of technology challenges existing legal systems, particularly concerning privacy and security in surveillance governance. Legal frameworks alone cannot resolve these issues. Continuous political dialogue, technical innovation, and institutional adaptation are needed. The EU's experience shows legal protections are necessary but not sufficient for managing digital surveillance challenges. The current paper also suggests improvements for EU digital surveillance law by focusing on three main areas. Firstly, the EU should strengthen implementation and enforcement by creating better mechanisms for monitoring compliance among member states, including regular assessments, technical assistance, and increased coordination between oversight bodies. Secondly, there should be enhanced cross-border cooperation in criminal investigations, ensuring compliance with fundamental rights and possibly requiring new agreements and standards for information sharing. Lastly, the EU needs more agile methods to handle privacy issues linked to new technologies. This could involve using regulatory sandboxes and creating adaptable legal frameworks to accommodate technological changes. The EU should improve transparency in surveillance by enhancing public reporting, parliamentary oversight, and protections for whistleblowers, while balancing operational security needs. Additionally, the EU should promote its surveillance governance model internationally and develop new frameworks for cooperation with countries having different legal and institutional systems, encouraging pragmatic collaboration on surveillance practices.

6.1 Future Research

This research highlights key trends shaping the future of surveillance governance. The development of surveillance technologies will necessitate legal responses to balance new capabilities with privacy risks. Global criminal activities demand international cooperation, and growing public awareness of privacy rights will exert pressure for stronger protections, even as security threats push for enhanced surveillance. The EU's experience with digital surveillance law offers useful lessons. Its focus on rights protection, judicial oversight, and proportionality provides a framework to address surveillance challenges while ensuring democratic accountability. However, the research shows that legal frameworks alone are insufficient to tackle the complexity of surveillance governance. The most important recommendation from the EU's approach is the need for continuous dialogue among stakeholders like law enforcement, privacy advocates, and technology companies. Landmark cases reveal that surveillance governance is as much about public debate and stakeholder engagement as it is about legal rulings. As surveillance technologies advance and new security issues arise, it becomes crucial to adopt an inclusive, democratic approach. The EU experience suggests that diverse legal and institutional arrangements should still rest on fundamental principles: rights protection, democratic accountability, and proportionality in security responses. Achieving a balance between

security and privacy is an ongoing effort, needing regular adjustments and a firm commitment to democratic values. The success of EU digital surveillance laws is contingent not just on the legal framework but also on the evolving political, social, and technological environment. Policymakers, courts, and civil society must ensure that surveillance governance continues to reflect democratic values and protect fundamental rights while addressing security needs in a complex, interconnected world.

References

[1] Agalliu P, Hoxha A. (2024) The European Union's AI Act: Guarding against or Employing Artificial Intelligence. Migration Letters . 2024;21(4):668–83. Available from: https://migrationletters.com/index.php/ml/article/view/7615

[2] Andenas M, Andenas M. (2003) Surveillance and data protection: regulatory approaches in the EU and member states. European Business Law Review . 2003 Dec 1;14(Issue 6):765–813. Available from: https://doi.org/10.54648/eulr2003038

[3] Birrer A, He D, Just N. (2023) The state is watching you—A cross-national comparison of data retention in Europe. Telecommunications Policy . 2023 Apr 5;47(4):102542. Available from: https://doi.org/10.1016/j.telpol.2023.102542

[4] Cauffman C, Goanta C. (2021) A new order: the Digital Services Act and Consumer protection. European Journal of Risk Regulation . 2021 Apr 15;12(4):758–74. Available from: https://doi.org/10.1017/err.2021.8

[5] *CCDCOE*. (2016). https://ccdcoe.org/incyder-articles/cjeu-declares-general-data-retention-unlawful-in-tele2-sverige/

[6] Columbia Global Freedom of Expression. (2023, November 11). *Schrems v. Data Protection Commissioner - Global Freedom of Expression*. Global Freedom of Expression. https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner

[7] Court of Justice of the European Union. (2014). Digital Rights Ireland and Others (Joined Cases C-293/12 and C-594/12**). https://eur-lex.europa.eu/legal-content/en/ALL/? uri=CELEX:62012CJ0293**

[8] Digital Rights Ireland 62012CJ0293. (n.d) Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293

[9] Directive (2016) 2016/680 - EN - Law Enforcement Directive; LED - EUR-LEX. Available from: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

[10] European Data Protection Supervisor. (2021) Study on the essence of the fundamental rights to privacy and to protection of personal data . 2021. Report No.: EDPS 2021/0932. Available from: https://www.edps.europa.eu/system/files/2023-11/edps-vub-study_on_the_essence_of_fundamental_rights_to_privacy_and_to_protection_of_personal_data_en.pdf

[11] European Papers. (2021). *Case Prokuratuur: Proportionality and the independence of authorities in data retention*. https://www.europeanpapers.eu/europeanforum/case-prokuratuur-proportionality-and-independence

[12] European Parliament. (2020) Data subjects, digital surveillance, AI and the future of work . 2020. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf

[13] European Union. (2006) DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL . Official *Journal of the European Union*; 2006. Report No.: L 105/54. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024

[14] Frontex as a hub for surveillance and data sharing: (2024) Challenges for data protection and privacy rights - 2024 – Gandhi

[15] GDPR Hub. (2024). *CJEU - C-203/15 and C-698/15 - Tele2 Sverige and Watson and Others*. https://gdprhub.eu/index.php?title=CJEU_-C%E2%80%91203/15_and_C%E2%80%91698/15-Tele2_Sverige_and_Watson_and_Others(Joined_Cases)

[16] Hendrix J. (2023) Tracking oversight of surveillance in the US and EU . Tech Policy Press. 2023b. Available from: https://www.techpolicy.press/tracking-oversight-of-surveillance-in-the-us-and-eu/

[17] Heyndels S. (2020) The age of surveillance capitalism. Tijdschrift Voor Philosophie . 2020 Jan 1;82(4). Available from: https://philpapers.org/rec/HEYTAO-2

[18] Ipr, I. (2025) How do the European Union's GDPR and China's PIPL regulate cross-border data flows? | International Policy Review . International Policy Review |. 2025. Available from: https://ipr.blogs.ie.edu/2025/01/27/how-do-the-european-unions-gdpr-and-chinas-pipl-regulate-cross-border-data-flows/

[19] Korff D. (2023) The lack of data on the effectiveness of mass surveillance. *SSRN Electronic Journal* . 2023 Jan 1; Available from: https://doi.org/10.2139/ssrn.4437119

[20] Langheinrich M. (2001) Privacy by design - Principles of Privacy-Aware Ubiquitous systems. Ubiquitous Computing . 2001 Sep 30;273–91. Available from: https://dx.doi.org/10.1007/3-540-45427-6_23

[21] McIntyre T. (2014) Challenging mass surveillance in Ireland and Europe. UCD Sutherland School of Law . 2014; Available from: https://www.ucd.ie/research/portal/t4media/CASE_STUDY_TJ_McIntyre_V2.pdf

[22] Ojazen T. (2017) Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In: Hart Publishing eBooks . 2017. Available from: https://doi.org/10.5040/9781509905447.ch-002

[23] Peers S, Hervey T, Kenner J, Ward A. (2014) The EU Charter of Fundamental Rights . Nomos eBooks. 2014. Available from: https://doi.org/10.5771/9783845259055

[24] Podkowik, J., Rybski, R., & Zubik, M. (2022). Judicial dialogue on data retention laws: A breakthrough for European constitutional courts? *International Journal of Constitutional Law*, *19*(5). https://academic.oup.com/icon/article/19/5/1597/6498025
[25] Power DJ. (2016) Big Brother can watch us. Journal of Decision System . 2016 Jun 10;25(sup1):578–88. Available from: https://doi.org/10.1080/12460125.2016.1187420
[26] Rønn KV, Lippert-Rasmussen K. (2020) Out of proportion? on surveillance and the proportionality requirement. Ethical Theory and Moral Practice . 2020 Jan 2;23(1):181–99. Available from: https://doi.org/10.1007/s10677-019-10057-z
[27] Scheinin M. (2015) EU-Funded Study: Electronic Mass Surveillance fails – Drastically . Just Security. 2015. Available from: https://www.justsecurity.org/16336/eu-funded-study-electronic-mass-surveillance-fails-drastically/
[28] *Schrems II landmark ruling: A detailed analysis*. (2020). United States | Global Law Firm | Norton Rose Fulbright. https://www.nortonrosefulbright.com/en-us/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis
[29] Tosza S. (2023) European Union · The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One? European Data Protection Law Review . 2023 Jan 1;9(2):163–72. Available from: https://doi.org/10.21552/edpl/2023/2/11
[30] Zwaan P, Schoenefeld JJ. (2024) Explaining different usages of policy monitoring in the EU. *Journal of European Integration*. 2024 Jun 5;1–17. Available from: https://doi.org/10.1080/07036337.2024.2354490