Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

Research Article

WHO AUTHORISES SURVEILLANCE? COERCIVE DIGITAL SURVEILLANCE, THE RULE OF LAW, AND ACCESS TO JUDICIAL OVERSIGHT: A CENTRAL AND EASTERN EUROPEAN PERSPECTIVE

Adem Ersin Bayra* and Nihat Bulut

DOI:
https://doi.org/10.33327/AJEE-18-9.4-a0002024

Date of submission: 26 Jul 2026
Date of acceptance: 18 Sep 2026
Online First Publication: 23 Oct 2026
Last Publication: 03 Nov 2026

Disclaimer:
The authors declare that their opinions and views expressed in this manuscript are free of any organisational impact.

Copyright:
© 2026 Adem Ersin Bayra and Nihat Bulut

ABSTRACT

Background: *Debates on digital surveillance are largely centred on privacy and data protection. However, the fundamental constitutional issue with coercive digital surveillance lies less in the severity of the interference than in who authorises it, and the oversight to which it is subject. In other words, the issues are essentially the separation of powers and access to justice.*

Method: *The study uses a comparative doctrinal approach. Four countries selected through purposive sampling, Poland, Hungary, Ukraine, and the United Kingdom, are analysed based on the European Parliament's PEGA Inquiry, the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), and reports by the European Commission.*

Results and Conclusions: *The shift of the authority to authorise surveillance from the legislature to the executive, and from there to lower-level administration and, increasingly, to private actors, has necessitated an examination of the authorisation architecture through four key hinges: the legislative reserve, independent prior authorisation, effective ex post oversight, and delegation safeguards. The study shows how digital surveillance challenges each hinge individually and how this manifests in the case study. The study's contribution lies in reframing digital surveillance primarily as a matter of authority allocation, identifying the four hinges of the authorisation architecture, and proposing a cumulative authorisation test tiered to the intensity of the intervention. Within this framework, access to justice becomes a prerequisite for legitimacy; the criterion, meanwhile, becomes transferable across different regimes. The case studies bear this out: in Poland and Hungary, all four hinges are failing simultaneously; in Ukraine, three are being rebuilt under EU accession conditionality; and in the United Kingdom, strengthening a single hinge is not enough to compensate for weakness in the others. The comparison shows that no matter how meticulously a proportionality review is conducted, it cannot correct a defect at the authorisation stage.*

1 INTRODUCTION

The revelation that the Pegasus spyware[1] was used against opposition politicians, lawyers, and journalists in Poland and Hungary in 2021 has brought digital surveillance back onto the agenda of European public law.[2] The debate has largely centred on the balance between privacy and the protection of personal data. However, the thought-provoking aspect of the incident is not the severity of the intrusion into an individual's private sphere, but rather the question of who authorises such an intrusion and to what (administrative or judicial) oversight it is subsequently subject. This is because this surveillance measure, which completely infiltrates the devices, such as telephones and computers, of the person under surveillance, has in many cases been implemented directly by security units attached to the executive, without independent judicial prior authorisation and without provision for effective *ex post* oversight. Yet, according to the established case law of the European Court

1 Pegasus is commercial spyware developed by the Israeli NSO Group that provides full access to a target device's microphone, camera, messaging apps, and location data without the owner's knowledge. The European Parliament's PEGA Committee of Inquiry investigated the use of this software in Europe between 2022 and 2023; the Committee found that the software was used systematically in Poland and Hungary against civilians, including opposition politicians, lawyers, and journalists. See European Parliament PEGA Committee, *Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware* (A9-0189/2023, 22 May 2023) paras 5, 18, 82, 111 <https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html> accessed 20 July 2026.

2 For the scope and European dimension of these revelations, see ibid.

of Human Rights (ECtHR), an intervention of this nature must, in principle, be subject to independent and, preferably, judicial prior review.[3]

However, the events in question go beyond isolated instances of abuse. They indicate a deeper, structural shift. Digital technologies are shifting what we term in this study the 'coercive surveillance authority' from the legislature to the executive, from high-level decision-making to lower-level administrative practice, and finally to private actors outside the public sector.[4] Indeed, the same trend has manifested itself in welfare state practices. Social welfare systems have evolved into interventionist algorithmic infrastructures that automatically profile citizens to verify eligibility and impose direct sanctions in the event of irregularities.[5] At this point, a privacy-centred approach can only see one side of the coin; it weighs up the severity of the intervention but often overlooks the institutional architecture that legitimises it, that is, by which body and through which procedure the authority is granted.

In this context, this study addresses digital surveillance not merely as a matter of rights violations, but as an issue of the constitutional allocation of authority and access to oversight. In this regard, the first question is not whether the intervention is proportionate, but who is constitutionally authorised to authorise it, and to what independent oversight the decision is subject. From this perspective, digital surveillance touches directly on the core of the separation of powers and access to justice.

The authorisation architecture rests on four hinges: the legislature sets the fundamental rule; an independent authority pre-approves the measure; implementation remains subject to effective *ex post* oversight and a right of appeal; and public accountability persists even when authority is delegated to private actors. Digital surveillance, however, challenges each of these hinges in turn. Bulk and automated authorisations reduce prior authorisation to a mere formality; 'black box' systems render *ex post* oversight ineffective; and the delegation of infrastructure to private providers disperses accountability.[6]

3 *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016) para 77 <https://hudoc.echr.coe.int/eng?i=001-160020> accessed 20 July 2026 (requirement for independent, preferably judicial, prior review).

4 Maarten Bouwmeester, 'Checks and Balances under Pressure in the Welfare State' (2025) 27(2) European Journal of Social Security 102-3 <https://doi.org/10.1177/13882627251330438> accessed 20 July 2026; Ryan Calo and Danielle Keats Citron, 'The Automated Administrative State: A Crisis of Legitimacy' (2021) 70(4) Emory Law Journal 832-3 <https://scholarlycommons.law.emory.edu/elj/vol70/iss4/1> accessed 20 July 2026. Regarding the transfer to private actors, see also Sarah Brayne, Sarah Lageson and Karen Levy, 'Surveillance Deputies: When Ordinary People Surveil for the State' (2023) 57(4) Law & Society Review 482 <https://doi.org/10.1111/lasr.12681> accessed 20 July 2026.

5 Philip Alston, *Report of the Special Rapporteur on Extreme Poverty and Human Rights* (UN Doc A/74/493, 11 October 2019) para 3 <https://docs.un.org/en/a/74/493> accessed 20 July 2026.

6 Regarding the reduction of prior authorisation to a mere token gesture, see Jennifer Cobbe, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making' (2019) 39(4) Legal Studies 643 <https://doi.org/10.1017/lst.2019.9> accessed 20 July 2026 (referring to the art 29 Working Party, emphasising that human oversight must be 'meaningful,

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

The literature on this subject is extensive but fragmented. The notion that authorising surveillance constitutes a separation-of-powers problem is not new. However, this debate has largely been reduced to a single question: whether the power to authorise should reside in the executive or the judiciary, and it has often been examined within a single legal system. In this vein, Clapham's emphasis on the separation of powers, Zalnieriute, Moses, and Williams's analysis of the rule-of-law values, Cobbe's critique of judicial review, and Brayne, Lageson, and Levy's analysis of proxy actors have each remained separate strands illuminating a single aspect. The contribution of this study lies in integrating these strands into a single, cumulative architecture of authorisation and linking this architecture to a tiered criterion based on the intensity of intervention.[7] Some of the studies examine the impact of automated decision-making on the rule of law.[8] Another part addresses the distortion of the balance of powers in favour of the executive, whilst yet another examines the surveillance regime of a specific country. Conversely, there is a gap in the literature for an integrated approach that does not limit the authorisation of coercive digital surveillance solely to the power to grant prior authorisation; that combines the legislative reserve, *ex post* oversight and special representatives within a single framework; that compares this in the context of Central and Eastern Europe and the European Union; and that proposes a workable standard.

The study's thesis is that intrusive digital surveillance can be legitimate only within a four-condition authorisation framework. In this context, first, the legislature must regulate the measure's fundamental framework in a manner that is accessible and foreseeable. Second, the measure must be subject to independent judicial or quasi-judicial prior authorisation. Third, the measure must be subject to effective *ex post* oversight and a right of appeal. Fourth, public accountability must be safeguarded even when authority is delegated to private actors. This study transforms these four conditions into a graduated criterion based on the intensity of the intervention, namely the 'legislative reserve, judicial prior authorisation, effective *ex post* oversight and appeal, and safeguards against delegation' test.

This study does not claim to replace the debate centred on privacy and proportionality. Rather, it points to a prerequisite that must be fulfilled beforehand. Before weighing the

rather than just a token gesture'). Regarding the rendering of human oversight ineffective in black-box systems, see Madalina Busuioc, 'Accountable Artificial Intelligence: Holding Algorithms to Account' (2021) 81(5) Public Administration Review 833 <https://doi.org/10.1111/puar.13293> accessed 20 July 2026 (the human intermediary becoming a 'hollow check' in automated decisions). Regarding the delegation to private providers and the fragmentation of accountability, see Brayne, Lageson and Levy (n 4) 482.

7 Nicholas Clapham, 'The Authorisation of Surveillance: A Separation of Power?' (*UK Constitutional Law Association Blog*, 25 June 2015) <https://ukconstitutionallaw.org/2015/06/25/nicholas-clapham-the-authorisation-of-surveillance-a-separation-of-power/> accessed 20 July 2026.

8 For a general overview, see Cobbe (n 6); Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82(3) Modern Law Review 425 <https://doi.org/10.1111/1468-2230.12412> accessed 20 July 2026.

severity of an intervention, it must be clear who authorised it and within which institutional framework. If this step is overlooked, the proportionality test risks obscuring the more fundamental question of authorisation.

The remainder of the study proceeds as follows: the second chapter sets out the study's aim, research questions, and methodology; the third chapter justifies why a shift from privacy to authorisation is necessary; and the fourth chapter analyses the four hinges of authorisation. In the fifth chapter, this analysis is applied to Central and Eastern Europe and the European Union; in the sixth chapter, a graduated framework is constructed. The seventh chapter addresses potential objections, while the eighth chapter presents our conclusions.

2 AIMS, RESEARCH QUESTIONS AND METHODOLOGY

In the context of coercive digital surveillance, the central issues, before any discussion of proportionality, are who grants the authority and under what institutional conditions. This study aims to transform these conditions into an evaluation criterion. This aim is articulated in two questions: (1) Under which institutional conditions can the authorisation of coercive digital surveillance be considered legitimate? (2) How do these conditions actually operate and erode across different types of European regimes?

The study adopts a comparative doctrinal approach, focusing on Central and Eastern Europe. This is because Poland and Hungary provide two examples where the politically motivated use of Pegasus intersects with a broader pattern of democratic backsliding.[9] Ukraine, meanwhile, holds particular significance in terms of its reform and European Union harmonisation process. ECtHR and CJEU case law form a common legal basis. The United Kingdom is considered a counter-example.

The four countries included in the comparison, Poland, Hungary, Ukraine, and the United Kingdom, were selected using a purposive sampling method, based on three complementary criteria. The first criterion is the adequacy of sources. In all four countries, documented and publicly available primary sources on authorisations for digital surveillance after 2020 exist.

The second criterion is the countries' legal position vis-à-vis the European safeguards regime. Poland and Hungary are EU Member States that, whilst subject to this regime, are eroding it from within. Ukraine, meanwhile, is a candidate country where efforts are being

9 For a conceptual framework on democratic backsliding, see Nancy Bermeo, 'On Democratic Backsliding' (2016) 27(1) Journal of Democracy 5 <https://doi.org/10.1353/jod.2016.0012> accessed 20 July 2026. On the use of Pegasus in Poland, see Marcin Rojszczak, 'EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses' (2021) 29(3-4) European Journal of Crime, Criminal Law and Criminal Justice 292-3 <https://doi.org/10.1163/15718174-bja10027> accessed 20 July 2026. Regarding Hungary, see European Parliament PEGA Committee, *Report* (n 1) paras 82, 83.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

made to establish the same safeguards from the outside. The United Kingdom, whilst outside the EU, is a stable legal system subject to European Convention on Human Rights (ECHR) scrutiny, with no signs of democratic regression.

The third criterion is that the sample must encompass both the 'most similar' and the 'most dissimilar' system designs. Poland and Hungary constitute the 'most similar' pair; both are members of the Visegrád Group[10] and the use of Pegasus has been documented in both. This pair demonstrates how all four 'hinges' can become dysfunctional simultaneously. Ukraine and the United Kingdom, in contrast, form the most dissimilar pair: in one, the accession process imposes reform pressure, while in the other, an established institutional balance prevails. This allows us to test whether the criterion applies only to democracies in decline.

The sources on which the analysis is based have also been selected in accordance with these criteria. For Poland and Hungary, we use the European Parliament's PEGA Inquiry and ECtHR case law; for the United Kingdom, the judicial and academic literature on the Investigatory Powers Act 2016; and for Ukraine, the European Commission's enlargement reports, and academic analyses. Primary sources (case law, legislation, and official reports) establish the normative framework of the criterion, while secondary literature explains how these hinges are eroded.

3 A SHIFT IN FRAMEWORK: FROM PRIVACY TO AUTHORISATION

Debates on digital surveillance are largely conducted in the language of privacy. This doctrine essentially asks: is the interference directed towards a legitimate aim and is it proportionate? However, this question assumes that authorisation has already been granted and merely discusses its limits. Yet questions precede this: 'who was constitutionally authorised to authorise this intervention?' and 'to what independent scrutiny was the decision subject?' This is, in fact, less a question of privacy than one of the separation of powers.[11] Moreover, underlying this is the principle of legality, which provides that rights and freedoms may only be restricted by law.[12] This principle also forms the basis for the legislative reserve discussed below.

10 The Visegrád Group is a regional cooperation platform established in 1991 by Poland, Hungary, the Czech Republic, and Slovakia to coordinate their integration into the EU and NATO. Today, the term also refers to the joint political and cultural grouping of these four countries.

11 For a contemporary theoretical analysis of the separation of powers, see Christoph Möllers, *The Three Branches: A Comparative Model of Separation of Powers* (OUP 2013) 8 <https://doi.org/10.1093/acprof:oso/9780199602117.002.0008> accessed 20 July 2026. For the classical formulation of the doctrine, see MJC Vile, *Constitutionalism and the Separation of Powers* (2nd edn, Liberty Fund 1998) 14. For the classical origins of the separation of powers, see Charles de Montesquieu, *The Spirit of the Laws* (Anne M Cohler, Basia C Miller, and Harold S Stone eds, CUP 1989) bk 11, ch 6.

12 For the principle that rights and freedoms may only be restricted by law (legality), see Council of Europe, *European Convention on Human Rights*: *as amended by Protocols 11, 14, and 15; supplemented by Protocols 1, 4, 6, 7, 12, 13, and 16* (ECtHR 2013) art 8(2) <https://www.echr.coe.int/

A privacy framework is necessary; however, it is insufficient on its own. Indeed, as Solove's detailed map also demonstrates, privacy theory provides a nuanced analysis of the harms caused by interference. However, the solution it offers, namely proportionality, data minimisation, and purpose limitation, operates after the authorisation decision.[13] Two regimes with the same privacy safeguards can differ entirely in terms of who authorises the surveillance. The privacy lens alone, however, cannot reveal this difference.

The first bridging concept that makes this difference visible is domination. Megiddo redefines the harm caused by unchecked digital power not as an intervention but as a form of domination.[14] Pettit's republican theory of non-domination, meanwhile, provides the normative foundation for this: what matters is not whether power is actually abused, but whether it is subject to control. In this respect, an unchecked capacity for surveillance constitutes domination, even if it is never abused. Indeed, it renders the citizen dependent on the arbitrary will of another.[15]

The second bridge is securitisation. As Graziani demonstrates, digital technologies normalise exceptional forms of governance by framing them as security practices. This framing shifts decision-making authority to the executive branch, to specialist units attached to the executive, such as border agencies, and to automated systems. Authority thus remains outside the scope of both democratic deliberation and judicial oversight.[16] In this way, securitisation explains which political mechanism is being used to bypass the architecture of authorisation.

The third dimension is private-sector power. In Zuboff's analysis, surveillance capacity is largely concentrated in commercial actors. When combined with domination and

documents/d/echr/convention_eng> accessed 20 July 2026; Charter of Fundamental Rights of the European Union (ratified 7 December 2000) [2012] OJ C 326/391, art 52(1) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT> accessed 20 July 2026. In the context of covert surveillance, this requirement is not satisfied by a purely formal legal basis alone; it also requires the 'quality of law', namely accessibility, predictability, and safeguards against arbitrariness. See *Malone v United Kingdom* App 8691/79 (ECtHR, 2 August 1984) paras 66, 67 <https://hudoc.echr.coe.int/fre?i=001-57533> accessed 20 July 2026; *The Sunday Times v United Kingdom* App 6538/74 (ECtHR, 26 April 1979) para 47 <https://hudoc.echr.coe.int/eng?i=001-57584> accessed 20 July 2026. However, the ECHR's concept of 'law' encompasses unwritten law and does not require a formal legislative monopoly; the legislative reserve argued for in this study derives not from this minimum standard of the Convention, but from the principle of the separation of powers.

13 Daniel J Solove, *Understanding Privacy* (Harvard UP 2008) 101-4 <https://ssrn.com/abstract=1127888> accessed 20 July 2026.

14 Tamar Megiddo, 'Online Activism, Digital Domination, and the Rule of Trolls' (2020) 58(2) Columbia Journal of Transnational Law 433-7 <https://dx.doi.org/10.2139/ssrn.3459983> accessed 20 July 2026.

15 Philip Pettit, *Republicanism: A Theory of Freedom and Government* (OUP 1997) 32 <https://doi.org/10.1093/0198296428.001.0001> accessed 20 July 2026.

16 Chiara Graziani, 'Technosecuritisation: Digital Technologies and the Securitisation of EU Migration Law' (2026) 28(1) European Journal of Migration and Law 35-6 <https://doi.org/10.1163/15718166-12340215> accessed 20 July 2026.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

securitisation, the question of 'who authorises' can be entirely removed from the realm of public law.[17] This point forms the theoretical backdrop to the 'shift to private actors' discussed in section 4.4.

Reframing the issue in terms of authorisation offers three advantages. First, it makes visible the shift of power between the branches of government and towards private actors. To put it more plainly, it reveals the shift in surveillance authority from the legislature to the executive and to private actors, that is, the shift in power underlying the question 'who authorises?'. Second, it links surveillance directly to the tradition of the rule of law and access to justice, which is particularly important in Central and Eastern Europe. Finally, it produces a transferable criterion for assessment across different regimes. This framework does not exclude privacy; on the contrary, it situates it within the context of a prior constitutional issue.[18] To put it more concretely, when a telephone is hacked using Pegasus, the main issue is not the extent to which privacy has been infringed. Rather, it is who authorised this measure and how much scrutiny is it subject to.

4 THE FOUR HINGES OF AUTHORISATION

The authorisation framework rests on four hinges, and digital surveillance challenges each of them individually. These hinges are addressed in turn under the four sub-headings below: the legislative reserve, independent prior authorisation, effective *ex post* oversight, and delegation to private actors. Each corresponds to one leg of the criterion to be established in Chapter Six.

4.1. Legislative Reserve

The first hinge of the authorisation architecture is the legislative reserve. A legislative body with democratic legitimacy must lay down fundamental and rights-restricting decisions about who may be monitored, on what grounds, and within what limits, through accessible and predictable rules. These decisions cannot be left entirely to the executive, nor can they be embedded within a technical framework. This requirement stems from both the 'quality of law' criterion sought by the ECtHR and the constitutional principle that fundamental matters fall within the remit of the legislature, in particular that rights and freedoms may be restricted only by law.

Case law clearly sets out this criterion. The ECtHR requires that secret surveillance regimes be based on a legal foundation that is accessible and foreseeable to the extent that it enables

17 Shoshana Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019) ch 18.

18 These three findings form the basis for the four-pronged analysis in ch. 4 and the graduated standard in ch. 6.

citizens to regulate their behaviour accordingly.[19] The CJEU also considers it essential that data retention and access regimes be governed by clear and precise rules.[20] The German Federal Constitutional Court, in its 1983 Census ruling, regarded the requirement that any interference with the processing of data be linked to a specific legal basis as a core safeguard of the right to informational self-determination.[21]

Digital surveillance erodes this foundation in two ways. First, rule-making authority shifts from the legislature to the executive. As Bouwmeester has demonstrated, in areas where automated systems are deployed, rule-making powers are increasingly being drawn towards the executive and are moving beyond the scope of legislative oversight.[22] Consequently, fundamental choices such as threshold values, targeting criteria and exceptions are shifting from legislation to administrative configuration.

Second, the rule itself is being transformed into 'code'. The operative norm is no longer the text of the law; it is the system's design, thresholds, training data, and model logic. Moreover, these choices are being made not by the legislature, but by developers and suppliers. As Calo and Citron emphasise, automation undermines the assumptions of expertise and accountability upon which the administration's legitimacy is based.[23] Yet, in a state governed by the rule of law, the authority to determine the fundamentals of the surveillance regime lies precisely with the legislature at this preliminary design stage.

This is not merely an abstract concern. In the context of the digital welfare state, automated systems have been implemented without their impact on fundamental rights being sufficiently debated in parliament.[24] Indeed, in the case of SyRI in the Netherlands, the regulation based on risk profiling was found by the courts to be in breach of Article 8 of the ECHR because it failed to meet the criteria of predictability and transparency. In other

19 *Roman Zakharov v Russia* App 47143/06 (ECtHR, 4 December 2015) paras 228, 229 <https://hudoc.echr.coe.int/fre?i=001-159324> accessed 20 July 2026; *Szabó and Vissy v Hungary* (n 3) para 59.

20 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* (CJEU, 8 April 2014) para 54 <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:62012CJ0293> accessed 20 July 2026; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* (CJEU, 6 October 2020) [2020] OJ C 433/3, para 132 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2020_433_R_0003> accessed 20 July 2026.

21 *Volkszählungsurteil* (German Federal Constitutional Court, 15 December 1983) BVerfGE 65/1, headnote 2 (3) and grounds (8) <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html> accessed 20 July 2026.

22 Bouwmeester (n 4) 102-3.

23 Calo and Citron (n 4) 803-4. For ensuring that the design is compatible with the rule of law and designers' accountability, see Zalnieriute, Bennett Moses and Williams (n 8) 443-4.

24 Alston (n 5) paras 3, 4, 43.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

words, the problem lies not in the implementation, but in the fact that the fundamental framework was not properly established by law from the outset.[25]

All this does not imply that any form of delegation of powers is problematic. The key point is that the fundamental choices determining the extent of the intervention must remain within the legislative reserve. Indeed, the approach taken by Enqvist and Naarttijärvi, which examines proportionality separately at each stage of automation, also supports this graduated logic.[26] The fact that the EU Artificial Intelligence Act (AI Act) sets fundamental limits[27] directly at the legislative level regarding certain forms of oversight provides a model worth following. Essentially, when the legislative reserve is eroded, the two hinges that follow it also lose their foundation. Oversight can operate only in relation to an existing rule.

4.2. Independent Prior Authorisation

The second hinge is independent approval, which applies before any intervention. The constitutional logic here is straightforward: the body seeking to monitor must not be the same as the body authorising the monitoring. Before any interventionist or coercive measure is implemented, an authority independent of the requesting body must approve it, in accordance with the criteria of necessity and proportionality, preferably a judicial body. However, the phrase 'preferably judicial' does not imply an absolute requirement for a court order; rather, it refers to the structural independence of the prior authorisation body from the unit carrying out the surveillance and the binding nature of its decision. Prior authorisation by an independent administrative authority whose decision is binding also meets this criterion. Prior authorisation is the threshold at which legality is tested before the intervention.

The ECtHR has consistently upheld this principle. In the Klass judgment, it stated that covert surveillance cannot be accepted without independent oversight.[28] In the Szabó and

25 Case C-09-550982 *NJCM and Others v The Netherlands (SyRI)* (District Court of The Hague, 5 February 2020) ECLI:NL:RBDHA:2020:1878 <https://www.julia-project.eu/database/case-law/241> accessed 20 July 2026; Rachovitsa and Niclas Johann, 'The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case' (2022) 22(2) Human Rights Law Review 5-6 <https://doi.org/10.1093/hrlr/ngac010> accessed 20 July 2026.

26 Lena Enqvist and Markus Naarttijärvi, 'Discretion, Automation, and Proportionality' in Markku Suksi (ed), *The Rule of Law and Automated Decision-Making* (Springer 2023) 160-70 <https://doi.org/10.1007/978-3-031-30142-1_7> accessed 20 July 2026.

27 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689, art 5 <http://data.europa.eu/eli/reg/2024/1689/oj> accessed 20 July 2026.

28 *Klass and Others v Germany* App 5029/71 (ECtHR, 6 September 1978) paras 55, 56 <https://hudoc.echr.coe.int/eng?i=001-57510> accessed 20 July 2026.

Vissy v. Hungary judgment, it found a regime in which a body subordinate to the executive authorised itself to be inadequate, as it lacked independent and, preferably, judicial prior review.[29] The Grand Chamber, in the Big Brother Watch judgment, required the oversight of an independent authority at every stage of mass data retention.[30]

Digital surveillance erodes this threshold in three ways. First, authorisation moves away from the individual and takes on a collective character. In this case, consent ceases to be a concrete decision directed at a specific person and becomes a blanket authorisation covering an entire category of data. Prior authorisation, meanwhile, is reduced to a mere formality. Indeed, as Porcedda demonstrates, courts occasionally legitimise this collective surveillance by approving the automated analysis of metadata themselves.[31]

Second, prior authorisation lacks independent and effective oversight. In the Pegasus case, security units subordinate to the executive in Poland implemented this measure, which completely infiltrates the device. Although access to the content of communications is formally subject to judicial authorisation, it has been established both in the case law of the ECtHR and in the European Parliament's PEGA Inquiry that effective and independent prior oversight is not in place.[32] It is precisely this structure that the Szabó and Vissy judgment rejected.

Third, remote access undermines the traditional logic of authorisation and search warrants. Ghappour shows that remote network searches conducted by law enforcement on the dark web shift the question of 'who decides' beyond the search-warrant framework. For when the location of the target is unknown, the competent authority required to grant authorisation also becomes unclear.[33]

A concrete example of what should be the case appears in recent EU legislation. Indeed, the EU AI Act generally prohibits real-time remote biometric identification for law enforcement purposes in public spaces. In the limited circumstances where it is

29 *Szabó and Vissy v Hungary* (n 3) para 85.

30 *Big Brother Watch and Others v the United Kingdom* Apps 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) para 356 <https://hudoc.echr.coe.int/fre?i=001-210077> accessed 20 July 2026.

31 Maria Grazia Porcedda, 'Automated Analysis in the AFSJ and Digital Single Market Monitoring: An Effaced Nexus' in Eleni Kosta and Irene Kamara (eds), *Data Retention in Europe and Beyond* (OUP 2025) 424 <https://doi.org/10.1093/9780191998980.003.0028> accessed 20 July 2026.

32 In the Polish regime, see Rojszczak, 'EU Criminal Law' (n 9) 299; see also Marcin Rojszczak, 'Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland' (2021) 17(1) Democracy and Security 4-7 <https://doi.org/10.1080/17419166.2020.1841367> accessed 20 July 2026. Regarding the failure of effective and independent prior review, see *Pietrzak and Bychawska-Siniarska and Others v Poland* Apps 72038/17 and 25237/18 (ECtHR, 28 May 2024) <https://hudoc.echr.coe.int/eng?i=002-14333> accessed 20 July 2026; and European Parliament PEGA Committee, *Report* (n 1), paras 27, 28.

33 Ahmed Ghappour, 'Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web' (2017) 69(4) Stanford Law Review 1079, 1082.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

permitted, the measure is subject to prior authorisation by a competent judicial authority or an independent administrative authority with binding decision-making powers, as well as an assessment of necessity and proportionality and a prior fundamental rights impact assessment.[34] Finally, the prior authorisation requirement is not only being weakened but is also shifting in nature. This is because it is increasingly private providers who are actually deciding on access requests.[35]

4.3. Ex Post Oversight and Effective Remedies: The Collapse of Access to Justice

The third hinge is the review that comes into play after the measure is implemented: the affected individual's ability to challenge the measure's legality before an independent authority, and the ability of review bodies to scrutinise its implementation meaningfully. This is, in fact, access to justice itself, the most concrete promise of the rule of law. In this study, access to justice is used primarily to mean effective judicial review and the right of appeal. Within this framework, the two concepts are considered complementarily. Digital surveillance and automated decision-making, however, undermine this promise in three respects.

The first of these is opacity. As machine learning-based systems rely on a complex web of calculations, the reasoning behind their decisions often cannot be explained to either the affected individual or the regulator. This 'black box' eliminates the conditions of justification and testability upon which judicial oversight relies.[36] The second is scale: whilst automated decisions are produced at an industrial pace, subsequent oversight operates on an individual basis and at a human pace. The third is the risk of diffusion of responsibility. When responsibility for a decision is divided among the designer, the supplier, the administration, and the final official, it becomes difficult to identify who to hold to account. As Busuioc emphasises, whilst this complexity does not absolve public administrators of responsibility, ensuring accountability in practice is becoming increasingly difficult.[37]

These dynamics are not abstract. In Australia's 'Robo-Debt' programme, a system that automatically matched income data wrongly charged hundreds of thousands of people. The programme's legality could not be effectively scrutinised for years, and the fault was only acknowledged after a major public and judicial backlash. Carney, who analyses the process through seven distinct failures, describes this collapse as 'the seven veils of failed guarantees of the rule of law'.[38]

34 Regulation (EU) 2024/1689 (n 27) arts 5(1)(h), 5(3), 27 (for the fundamental rights impact assessment).

35 Porcedda (n 31) 423-4.

36 Calo and Citron (n 4) 830-2; Cobbe (n 6) 636-8.

37 Busuioc (n 6) 829-30.

38 Terry Carney, 'Robo-Debt Illegality: The Seven Veils of Failed Guarantees of the Rule of Law?' (2019) 44(1) Alternative Law Journal 4-5 <https://doi.org/10.1177/1037969X18815913> accessed 20 July 2026.

The child benefit scandal in the Netherlands (Toeslagenaffaire) also exhibits a similar pattern. Automated risk profiling wrongly labelled thousands of families as suspected of irregularities. Neither the administrative courts nor parliament recognised the problem for years. Bouwmeester demonstrates that the root cause of the collapse lies not in automation itself, but in its combination with rigid welfare conditionality, that is, the linking of access to benefits to increasingly onerous conditions, intensive monitoring, and strict sanctions, coupled with the executive's tendency to disregard constitutional checks and balances.[39]

The problem is not unique to social welfare administration. In the United Kingdom, the expansion of surveillance and security powers has gone hand in hand with the erosion of effective accountability amid rights violations. In this context, Webber has examined the process of expanding digital surveillance capacity in the United Kingdom under the heading of 'institutionalised impunity'.[40] The common thread running through all these examples is that, whilst *ex post* oversight exists in form, it has been hollowed out in practice.

As regards access to justice, the issue is two-fold. An effective remedy requires not only the existence of a court, but also the ability of the affected person to substantiate their claim, that is, to have access to the grounds for the decision. Opacity, however, undermines the 'equality of arms' that is essential at this stage. As Enqvist and Naarttijärvi have demonstrated, proportionality reviews must be carried out separately at different stages of automation, and no stage should be entirely devoid of human judgement.[41] For this reason, the right to an explanation and the right to human intervention are not merely formal safeguards, but prerequisites for the functioning of *ex post* oversight.[42]

This breakdown is particularly evident in Central and Eastern Europe. The requirement for judicial oversight in the covert surveillance regime, established by the Polish Constitutional Tribunal's judgment K 23/11 (2014), has been eroded by subsequent legislative measures. With the Tribunal rendered ineffective, an effective *ex post* oversight body under domestic law has, in practice, ceased to exist. The ECtHR confirmed this pattern in its judgment in Pietrzak and Bychawska-Siniarska v. Poland, finding three separate violations of Article 8 of the Convention in relation to Poland's operational control regime, the retention and use of communications data, and the covert surveillance regime under the Counter-Terrorism Act.[43] The judgment constitutes a direct and concrete confirmation of the collapse of access to justice, in that it accepts on its merits the applicants' claim that the oversight of the secret services is illusory. Indeed, the Court identifies a fundamental flaw: national law lacks an effective remedy capable of challenging the legitimacy of the surveillance measure.

39 Bouwmeester (n 4) 112-3.

40 Frances Webber, 'Impunity Entrenched: The Erosion of Human Rights in the UK' (2022) 63(4) Race & Class 60 <https://doi.org/10.1177/03063968221083193> accessed 20 July 2026.

41 Enqvist and Naarttijärvi (n 26) 168.

42 Paweł Szwajdler, 'Automated Judicial Decision-Making Systems and New Legal Principles' [2026] Constitutional Political Economy 13 <https://doi.org/10.1007/s10602-025-09490-3> accessed 20 July 2026.

43 *Pietrzak and Bychawska-Siniarska and Others v Poland* (n 32).

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

CJEU case law also supports this line of reasoning. The Court has required not only prior limitations but also independent *ex post* oversight and an effective remedy in regimes governing the mass storage and access to data. Notification is the de facto prerequisite for this chain. Indeed, if the data subject is not informed within the earliest reasonable time after the surveillance has ended, the right of appeal will remain merely theoretical.[44] However, there is a fundamental point highlighted in this section. Namely, however robust *ex post* oversight may be, it is not sufficient on its own. In the Robo-Debt and Toeslagenaffaire cases, the courts have finally acted. However, by the time this stage is reached, irreparable damage has already been done.

4.4. The Role of Private Actors

The fourth hinge concerns authority delegation. Even if private actors effectively perform coercive oversight, public accountability must be safeguarded. Yet digital surveillance is increasingly transferring this function to operators, platforms, technology suppliers, and even ordinary citizens. This creates an accountability gap that falls outside the scope of public law oversight.

The private actors to whom authority has been delegated fall into four categories. The first are the infrastructure providers who actually implement storage and access orders and act as gatekeepers at the point of access to data. The second are the technology suppliers who design the system's operating rules, that is, its thresholds and logic. The third are ordinary individuals carrying out surveillance on behalf of the state. Indeed, Brayne, Lageson, and Levy refer to these as 'surveillance agents', whilst Borges Monroy analyses this network as a delegated order.[45] Fourth, there is the self-governance of technology itself. As Eisenberger demonstrates, technological self-governance can erode the conditions of the rule of law by shifting norm-setting from the public sphere to private design.[46]

This mechanism often remains invisible. Porcedda demonstrates that whilst courts and EU law assign a custodial role to private electronic communications and information society services, this role becomes obscured in legal analysis. This is because the private

44 Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Schrems* (CJEU, 16 July 2020) paras 186, 187 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311> accessed 20 July 2026; Charter of Fundamental Rights of the European Union (n 12) art 47. For the post-measure notification obligation, see *Roman Zakharov v Russia* (n 18) paras 286–288; *Szabó and Vissy v Hungary* (n 3) para 86.

45 Brayne, Lageson and Levy (n 4) 482; Isadora Borges Monroy, 'The Surveillance Complex: Deputised Law and Order in Advanced Democracies' [2025] Information, Communication & Society 4 <https://doi.org/10.1080/1369118X.2025.2505696> accessed 20 July 2026.

46 Iris Eisenberger, 'Technology's Self-Governance' in Roger Brownsword and Larry A DiMatteo (eds), *The Cambridge Handbook of the Governance of Technology* (CUP 2026) 34 <https://doi.org/10.1017/9781009522519.004> accessed 20 July 2026.

actor making critical access decisions operates without being bound by the authorisation framework of public law.[47]

Legislation, meanwhile, reinforces this shift: the e-Evidence Regulation, which has applied since 18 August 2026, directs cross-border electronic evidence orders (European Production and Preservation Orders) directly to private providers and designates them as the enforcing parties. Consequently, the executing state's cross-border judicial intermediary role is bypassed, and the burden of actually facilitating access, along with the decision whether to authorise access, falls squarely on the private provider.[48] Zuboff's analysis of surveillance capitalism also serves as a reminder that this private power has risen not merely to an instrumental role, but to a rule-setting position.[49]

5 COMPARATIVE APPLICATION: CENTRAL AND EASTERN EUROPE AND THE EU AXIS

When applied to different regimes, the four hinges break down in various ways. Bermeo's 'democratic backsliding taxonomy' clarifies this analysis. According to this, contemporary backsliding does not occur through a coup, but through the covert and gradual expansion of executive power.[50] Digital surveillance, meanwhile, serves as both a means and an indicator of this expansion, and is becoming most acutely visible in Central and Eastern Europe, where the rule of law is under pressure. The country profiles in this section are based on legislation and case law in force in July 2026.

Poland and Hungary are paradigmatic examples. The European Parliament's PEGA inquiry has established that various EU governments have used Pegasus and similar spyware against journalists, politicians, and public officials, and that this poses a threat to the principles of democracy and the rule of law.[51] The issue rests on four hinges: the measure lacks a clear legal basis (4.1). Security agencies under the executive branch are authorising their own actions without independent judicial prior authorisation (4.2). *Ex post* oversight remains

47 Porcedda (n 31) 424, 449.

48 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings [2023] OJ L 191/118, rec 9, art 10 <http://data.europa.eu/eli/reg/2023/1543/oj> accessed 20 July 2026. For the position of the Pegasus supplier, see Rojszczak, 'EU Criminal Law' (n 9) 315-6.

49 Zuboff (n 17) ch 18, pt IV.

50 Bermeo (n 9) 10-1.

51 European Parliament Recommendation of 15 June 2023 to the Council and the Commission Following the Investigation of Alleged Contraventions and Maladministration in the Application of Union law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2023/2500(RSP)) [2024] OJ C 2024/494, paras 14, 17 <http://data.europa.eu/eli/C/2024/494/oj> accessed 20 July 2026. For detailed findings, see European Parliament PEGA Committee, *Report* (n 1).

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

merely formal (4.3). The private contractor establishing the technical capacity, meanwhile, is beyond the scope of accountability (4.4). As regards Hungary, the Szabó and Vissy judgment[52] found this structure to be in breach of the Convention.

Poland illustrates the extent of this erosion. As early as 2014, in its ruling K 23/11, the Polish Constitutional Tribunal (Trybunał Konstytucyjny) found the regime governing covert surveillance and access to stored data to be partially unconstitutional and imposed a requirement for judicial oversight. However, subsequent legislation eroded these safeguards; the oversight required for access to communications content has weakened since 2016, and this process has coincided with the period during which the ruling party rendered the Constitutional Tribunal ineffective.[53] Indeed, in 2024, the ECtHR once again found Poland's covert surveillance legislation to be in breach of the Convention.[54] This overlap is particularly evident in the context of Central and Eastern Europe: an executive branch that renders the courts ineffective also tends to expand its surveillance powers. Consequently, subsequent judicial review is doubly weakened due to both a lack of transparency and the erosion of judicial independence. The CJEU has also addressed the undermining of judicial independence in Poland as a rule of law issue.[55] In conclusion, the most critical issue for access to justice is that the court to which a victim of surveillance can turn has been weakened by the authorities responsible for expanding surveillance.

Ukraine is in a unique position: as a candidate country, it is in the middle of the EU accession process, yet it operates under ongoing martial law conditions. The European Commission's 2024 Enlargement Report highlights concrete issues in three of the hinges of the authorisation framework. On the legislative reserve, parliamentary oversight has largely been confined to closed meetings and has effectively become dysfunctional. Regarding

52 *Szabó and Vissy v Hungary* (n 3) (breach of art 8; operative part of the judgment).

53 During the 2015–2016 period, the ruling party (PiS) prevented judges who had been lawfully elected from taking up their posts at the Constitutional Court and appointed its own candidates; it subsequently rendered the Court largely ineffective through regulations that made its decision-making process more cumbersome (requiring a qualified majority, hearing cases solely in the order in which they were received, and a high quorum for meetings) and by failing to publish certain of the Court's decisions in the Official Gazette. With the appointment of a president close to the government at the end of 2016, the Court effectively lost its status as an independent oversight body. For a detailed analysis, see Wojciech Sadurski, *Poland's Constitutional Breakdown* (OUP 2019) ch 3 (The remaking of the Constitutional Tribunal; judicial appointments 64-70, non-publication of decisions 75-7 and 93-4).

54 Case K 23/11 (Polish Constitutional Tribunal, 30 July 2014); see Agnieszka Grzelak, 'Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11' (2016) 22(3) European Public Law 479-82 <https://doi.org/10.54648/euro2016030> accessed 20 July 2026; *Pietrzak and Bychawska-Siniarska and Others v Poland* (n 32) (breach of art 8 in regimes of covert surveillance, data retention and access).

55 Case C-619/18 *European Commission v Republic of Poland* (CJEU, 24 June 2019) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0619> accessed 20 July 2026. (Irremovability and independence of judges; art 19(1) TEU). For an analysis of the EU's intervention, see Sadurski (n 53) ch 8 ('Europe to the Rescue').

independent prior authorisation, the National Anti-Corruption Bureau of Ukraine (NABU), the main anti-corruption investigative body, has been deprived of its autonomous wiretapping capabilities, making the authorisation decision dependent on other authorities. As regards access to justice, concerns about the rule of law and press freedom have been raised over surveillance practices targeting journalists in government-controlled regions. The main pressure in rebuilding these hinges stems from the rule of law conditionality attached to the country's candidate status by the EU.[56]

EU law is the common ground across these national landscapes. The CJEU's case law on data retention and access, the Law Enforcement Directive, the EU AI Act and the e-Evidence Regulation (applicable since 18 August 2026) provide a supranational authorisation framework binding on member states and candidate countries.[57] The gap between European Union standards and national implementation, however, is the fault line of the rule of law. Compliance with the European Union also constitutes the primary lever for closing this gap.

The United Kingdom stands as a counter-example outside this framework. The Investigatory Powers Act of 2016, which followed the Anderson Report,[58] introduced a 'double lock' model that combines ministerial approval for surveillance authorisation with the approval of an independent judicial commissioner.[59] Thus, the executive's monopoly on prior authorisation was broken for the first time. However, during the same period, surveillance powers were expanded and effective accountability was eroded.[60] Even the Grand Chamber's

56 On the EU's rule of law conditionality and Ukraine, see Maryna Rabinovych, 'EU Enlargement Policy Goes East: Historical and Comparative Takes on the EU's Rule of Law Conditionality vis-à-vis Ukraine' (2024) 16 Hague Journal on the Rule of Law 715 <https://doi.org/10.1007/s40803-024-00223-6> accessed 20 July 2026. For concerns regarding monitoring during wartime, see European Commission, *Ukraine 2024 Report* (SWD(2024) 699, 30 October 2024) 30, 35, 40 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024SC0699> accessed 20 July 2026

57 Joined Cases C-293/12 and C-594/12 (n 20); Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (CJEU, 21 December 2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0203> accessed 20 July 2026; Joined Cases C-511/18, C-512/18 and C-520/18 (n 20); Directive (EU) 2016/680; Regulation (EU) 2024/1689 (n 27) annex III; Regulation (EU) 2023/1543 (n 48) arts 9, 10. For the impact of EU data retention case law on national regimes, see Eurojust, *The Effect of Court of Justice of the European Union Case-Law on National Data Retention Regimes and Judicial Cooperation in the EU* (European Union 2024) pt 4.3 <https://doi.org/10.2812/2621651> accessed 20 July 2026.

58 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (*GOV.UK*, 11 June 2015) <https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review> accessed 20 July 2026. — An independent reform report that comprehensively reviewed the UK's surveillance powers and recommended that all warrants be subject to authorisation by Judicial Commissioners.

59 Clapham (n 7); UK Investigatory Powers Act (2016) s 23 ("double lock", authorisation by Judicial Commissioners) <https://www.legislation.gov.uk/ukpga/2016/25/contents> accessed 20 July 2026.

60 *Big Brother Watch and Others v the United Kingdom* (n 30) (s 8(4) bulk interception regime's breach of Art 8; operative paragraph).

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

finding of a breach of the Convention in the Big Brother Watch judgment failed to prevent the erosion of internal accountability.[61] Indeed, the 2024 amending legislation enacted following the judgment introduced a new regime for bulk datasets with low privacy expectations, thereby expanding surveillance powers.[62] The United Kingdom thus serves both as proof that pre-authorisation reform is feasible and as a warning that strengthening a single hinge is insufficient to safeguard the others. This reinforces the study's central argument that conditions must be assessed cumulatively.

One further point should be added at this stage. Indeed, including the United Kingdom in the sample serves as a test not only in terms of regime type (EU member, candidate, non-member) but also in terms of differences in legal systems (common law or civil law tradition). Although the four-hinged architecture is framed in the terminology of continental European public law, institutional equivalents in the United Kingdom, such as the 'double lock' and the Investigatory Powers Tribunal, demonstrate that the criterion's portability extends beyond regime type to encompass legal traditions as well.

6 AUTHORISATION ARCHITECTURE: A GRADUATED STANDARD

The preceding sections point to a common conclusion: the legitimacy of coercive digital surveillance cannot be reduced to a single proportionality test. Proportionality review is, of course, necessary. However, it operates both after the authorisation decision has been made and remains largely undefined. This section aims to establish a structural criterion before the proportionality assessment. Under this criterion, legitimacy depends on the simultaneous fulfilment of four cumulative conditions, and the threshold for each rises with the intensity of the intervention. Who decides which tier a measure falls into is also part of this framework.[63] Indeed, this determination is made not by the unit requesting the measure, but by the pre-approval authority. They operate in sequence rather than in competition. The four conditions determine whether the authorisation is constitutionally available; proportionality then governs how an authorised measure is applied in the individual case. A favourable proportionality assessment cannot rescue a measure that fails the authorisation test, whereas one that passes it remains fully subject to proportionality review at every stage.

61 For a general discussion of the erosion of rights and accountability in the United Kingdom, see Webber (n 40) 60.

62 UK Investigatory Powers (Amendment) Act (2024) <https://www.legislation.gov.uk/ukpga/2024/9/contents> accessed 20 July 2026.

63 This model of four cumulative conditions is a proposal put forward in this study, developed with inspiration from the four-stage distinction in Enqvist and Naarttijärvi's proportionality analysis (legislative, systemic, decision-making and ex post proportionality); see Enqvist and Naarttijärvi (n 26).

The logic behind the criterion we have established is straightforward. Where proportionality alone is insufficient, we need a concrete tool to complement it. This study establishes that tool as a criterion that classifies the supervisory measure into four tiers according to the intensity of the intervention and assesses the four conditions with progressively greater rigour at each tier. The following paragraphs first define these four levels. The four conditions are set out individually, followed by an illustration of the criterion's cumulative and tiered operation using an example, and finally, it is applied to three specific measures.

The scaling variable is intervention intensity. Within this framework, four levels can be distinguished: Level 1, targeted access to metadata; Level 2, the interception of targeted content and communications; Level 3, bulk or automated analysis; and Level 4, device infiltration, equipment tampering, and real-time biometric identification. As the level increases, each of the four conditions listed below becomes more stringent.[64]

In this regard, the first condition is the legislative reserve. Primary legislation must lay down fundamental rules; as the level increases, the law must also be more certain. The minimum safeguards required by the ECtHR about covert surveillance, namely, the definition of offences and categories of persons, time limits, and rules governing examination, use, storage, and destruction, provide a concrete measure of this clarity.[65]

The second condition is independent prior authorisation. At lower levels, an independent administrative authority issuing binding decisions may suffice. However, at higher levels, an independent judicial body must grant authorisation, following an individual assessment specific to the person concerned and a concrete examination of the criteria of necessity and proportionality. In this context, the prior authorisation model established by the EU AI Act for real-time biometric identification is a concrete example of the standard required at the higher level.[66]

The third condition is effective *ex post* oversight and redress. The data subject must be notified where possible; must have access to the reasoning behind the decision; and must have recourse to an independent supervisory body and an effective judicial remedy. In the case of automated and bulk processing, this condition also encompasses systemic auditability and the rights to explanation and human intervention.[67]

64 For a comparative example of a tiered regulatory architecture based on risk intensity, see Regulation (EU) 2024/1689 (n 27) arts 5, 6 et seq.

65 *Weber and Saravia v Germany* App 54934/00 (ECtHR, 29 June 2006) para 95 <https://hudoc.echr.coe.int/eng?i=001-76586> accessed 20 July 2026; *Roman Zakharov v Russia* (n 19) para 231.

66 Regulation (EU) 2024/1689 (n 27) arts 5(1)(h), 5(3); *Klass and Others v Germany* (n 28) para 51; *Szabó and Vissy v Hungary* (n 3) para 77.

67 Charter of Fundamental Rights of the European Union (n 12) art 47; Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (CJEU, 16 July 2020), paras 186, 187 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311> accessed 20 July 2026. For the rights to explanation and human intervention, see Szwajdler (n 42) 33-5; Busuioc (n 6) 825-8; Cobbe (n 6) 641.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

The fourth and final condition concerns safeguards for delegating authority. Where authority is delegated to private actors, public law obligations, namely transparency, accountability, responsibility, and independent oversight, must be transferred along with the authority.[68]

Together, these four conditions operate in two ways, both cumulatively and progressively. Consequently, the proposed criterion is two-dimensional. In this respect, each condition must be met collectively, while the threshold for each rises in line with the intensity of the intervention. Failure to meet any one condition negates the measure's legitimacy at that level. The threshold, meanwhile, rises in line with the intensity of the intervention. For example, Pegasus is classified at the highest level (Level 4) because it fully infiltrates the device. In this respect, it fails to meet all four conditions; indeed, it lacks a clear legal basis, independent judicial prior authorisation, and effective *ex post* oversight. Furthermore, the supplier remains entirely outside any accountability mechanism.[69]

In contrast, targeted access to metadata, which remains at Level 1 due to its narrow scope, can satisfy the criterion with less onerous requirements. This demonstrates that the criterion is not an outright ban, but a graduated threshold of legitimacy.

Table 1. **Application of the authorisation criterion by tier**

Condition	Targeted measure (Levels 1–2)	Bulk / automated / device intrusion (Levels 3–4)
Legislative reserve	Clear legal basis; definition of offence and person categories	In addition: detailed specification in law of thresholds, time limits, data types, and destruction rules
Independent prior authorisation	Independent administrative or judicial prior authorisation; necessity and proportionality	Individualised judicial prior authorisation; additional safeguards throughout the process in the case of blanket authorisation
Effective *ex post* oversight	Notification (where possible) and effective judicial remedy	In addition: independent supervisory body, systemic accountability, right to explanation and human intervention
Proxy safeguards	Legal/contractual liability for the private actor taking over	In addition: transparency, auditability, and independent oversight of the private actor

68 Porcedda (n 31) 423-5, 436; Eisenberger (n 46) 22-5.

69 European Parliament, *Investigation of the Use of Pegasus and Equivalent Surveillance Spyware* (PE 747.923, 7 June 2023) <https://www.europarl.europa.eu/thinktank/mt/document/EPRS_ATA(2023)747923> accessed 20 July 2026; Rojszczak, 'EU Criminal Law' (n 9) 290-300.

Applying the table to the Pegasus case concretely demonstrates the criterion's diagnostic function. As the measure is classified at the highest level (Level 4) due to its complete infiltration of the device, it is subject to the strict conditions set out in the second column of the table. In the Polish implementation, none of the four conditions was met. Regarding the legislative scope, the threshold, duration, and data type are not tied to a detailed legal framework. With regard to independent prior authorisation, no individualised judicial authorisation has been obtained.

Regarding *ex post* oversight, neither notification nor an effective remedy has been implemented. As for safeguards regarding the provider, the supplier has been exempted from transparency and auditability obligations. Taken together, these four shortcomings, under the criterion we propose, undermine the regime's legitimacy. Of these shortcomings, the inadequacy of the legal framework, independent prior authorisation and *ex post* oversight has also been explicitly recognised by the ECtHR in its judgment in Pietrzak and Bychawska-Siniarska v. Poland as grounds for a violation of Article 8.[70]

In this context, the criterion can be illustrated using three examples. The first example concerns the retention and subsequent retrieval of mass communications metadata, which falls under Level 3 (mass/automated analysis). Here, the legislative framework must provide the clear and precise rules required by the CJEU, with prior authorisation requiring an independent authorisation for each access request, whilst *ex post* oversight requires notification and an effective remedy. Unless these safeguards are in place, the regime cannot be considered legitimate, however 'proportionate' it may be presented. The second example is real-time facial recognition in public spaces, which falls under the highest tier, namely Tier 4. The measure is subject to the threshold established by the AI Act (judicial or administrative prior authorisation, strict temporal and spatial limits, and a prior fundamental rights impact assessment). If this threshold is not met, the measure cannot be authorised. The third example is personalised, targeted interception of communications based on a court order. This may be lawful under Level 2 with standard minimum safeguards.[71]

The principle of legitimacy underpinning this criterion is non-domination: an unchecked surveillance capacity is not legitimate, even if it is never abused. For it renders the citizen dependent on an arbitrary will.[72] The third condition ensures access to justice, whilst the criterion offers a doctrine that is transferable across different types of regimes without being tied to a specific constitutional order.

70 *Pietrzak and Bychawska-Siniarska and Others v Poland* (n 32).

71 Joined Cases C-293/12 and C-594/12 (n 20) on metadata retention and the Court of Justice's minimum conditions and Joined Cases C-511/18, C-512/18 and C-520/18 (n 20). For real-time biometrics, see Regulation (EU) 2024/1689 (n 27) arts 5(1)(h), 5(3). For traditional minimum safeguards, see *Weber and Saravia v Germany* (n 65) para 95.

72 Pettit (n 15) 22. For end-to-end safeguards in bulk interception, see *Big Brother Watch and Others v the United Kingdom* (n 30) paras 350–360.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

7 OBJECTIONS AND LIMITATIONS

The proposed criterion must pre-emptively address the four anticipated objections. The first of these is the objection about security and efficiency: surveillance saves lives, whilst structural conditions paralyse law enforcement. The response to this is as follows: the criterion does not prohibit surveillance but merely channels it. Emergencies can be addressed both through the tiered structure and via exceptional procedures of the kind envisaged by the EU AI Act.[73]

The second objection is that the courts already carry out proportionality reviews. However, proportionality presupposes a valid authorisation and only applies thereafter. The criterion, in contrast, prioritises the structural question that precedes it. Indeed, the fact that the ECtHR itself supplements proportionality with minimum safeguards confirms this priority.[74]

The third objection is that the legislature cannot keep pace with rapid technological change. In response, the 'reserved sphere' encompasses fundamental choices rather than technical details. Certainty is a gradual process, and a legitimate delegation of authority is possible with safeguards. The issue is not merely delegation of powers, but preventing the legislature from effectively abdicating its duty to set fundamental limits. Indeed, Enqvist and Naarttijärvi also emphasise that proportionality review must begin at the legislative stage, and that a legal framework failing to provide minimum safeguards will create a lack of proportionality across the entire system.[75]

The fourth objection is that Poland, Hungary, Ukraine, and the United Kingdom cannot be compared. However, the criterion asks the same four structural questions, irrespective of the regime. In this respect, it is not a means of substantive harmonisation, but rather a diagnostic tool. Consequently, the differences are not a flaw, but a finding in their own right. It is also necessary to note a limitation of the comparison: the findings regarding Ukraine are largely based on reports from EU institutions. To that extent, they warrant caution.

Finally, we must acknowledge a limitation. The framework regulates authorisation. Whether a particular form of surveillance should exist at all, that is, substantive red lines, is a separate issue. Indeed, the fact that the EU AI Act prohibits certain applications, such as social scoring for law enforcement purposes or real-time remote biometric identification in public spaces, demonstrates that some measures cannot be legitimate even if authorised.[76]

73 For the emergency use procedure, see Regulation (EU) 2024/1689 (n 27) art 5(3).

74 *Roman Zakharov v Russia* (n 19) paras 231, 232; *Weber and Saravia v Germany* (n 65) para 95.

75 Enqvist and Naarttijärvi (n 26) 161-3.

76 For prohibited applications, see Regulation (EU) 2024/1689 (n 27) art 5(1).

8 CONCLUSION

The constitutional question is not whether we are being monitored. The real issues are who authorises the monitoring and what checks and balances are in place for this decision. Shifting the focus away from privacy and treating digital surveillance as a matter of allocating authority and access to justice brings to light the wound that the lens of privacy overlooks. The crux of the matter lies not in the surveillance of the individual, but in where the will that commands this surveillance originates and to what limits it is bound. Assessing the gravity of a privacy breach remains incomplete insofar as it overlooks the institutional chain that lends legitimacy to that breach: the decision-making body, the authority that grants prior authorisation, and the body that carries out subsequent oversight.

On this basis, the study proposes a graduated authorisation criterion. Accordingly, four cumulative conditions have been established, with thresholds that tighten in line with the intensity of the intervention. The four conditions are: the legislative reserve (where fundamental choices are subject to democratic representation), independent prior authorisation (separation of the authorising body from the authorised body), effective *ex post* oversight and recourse (judicial review of the decision), and safeguards of representation (public accountability even in the case of delegation to the private sector), which collectively ensure both democratic legitimacy before authorisation and access to justice thereafter. This criterion makes access to justice a prerequisite for legitimacy and has transferable value across regimes. Harmonisation with the European Union serves as the primary lever for re-establishing this architecture in Central and Eastern Europe. The question of who can authorise the surveillance state concerns the rule of law itself.

Through a study of four countries selected using purposeful sampling, this research has revealed the four hinges of this authorisation architecture and how digital surveillance strains each of them. Examples from Central and Eastern Europe show that this architecture is progressively eroded along a continuum. Pegasus, meanwhile, has shown that, at the end of the spectrum, all four hinges can collapse simultaneously. The UK example, conversely, illustrates the same lesson: strengthening a single hinge (the 'double lock' model) was insufficient to protect the others; even being a party to the Convention and the Grand Chamber's finding of non-compliance failed to prevent the erosion of internal accountability.

A limitation of this study must also be clearly stated here. The proposed framework is structural-normative in nature. A detailed case study concerning national constitutional court rulings, specific Pegasus deployments, or the actual functioning of independent oversight bodies falls outside the scope of this study. Future studies could examine how national supreme courts address the authorisation architecture through doctrinal case studies, and the effectiveness of independent pre-approval and *ex post* oversight bodies through empirical research. How national courts interpret the biometric authorisation regime under the EU AI Act is also a fruitful area to monitor. The proposed criteria enable these future studies to use a common analytical framework.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

REFERENCES

1. Alston P, *Report of the Special Rapporteur on Extreme Poverty and Human Rights* (UN Doc A/74/493, 11 October 2019) <https://docs.un.org/en/a/74/493> accessed 20 July 2026
2. Anderson D, *A Question of Trust: Report of the Investigatory Powers Review* (*GOV.UK*, 11 June 2015) <https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review> accessed 20 July 2026
3. Bermeo N, 'On Democratic Backsliding' (2016) 27(1) Journal of Democracy 5 <https://doi.org/10.1353/jod.2016.0012> accessed 20 July 2026
4. Borges Monroy I, 'The Surveillance Complex: Deputised Law and Order in Advanced Democracies' [2025] Information, Communication & Society 1 <https://doi.org/10.1080/1369118X.2025.2505696> accessed 20 July 2026
5. Bouwmeester M, 'Checks and Balances under Pressure in the Welfare State' (2025) 27(2) European Journal of Social Security 98 <https://doi.org/10.1177/13882627251330438> accessed 20 July 2026
6. Brayne S, Lageson S and Levy K, 'Surveillance Deputies: When Ordinary People Surveil for the State' (2023) 57(4) Law & Society Review 462 <https://doi.org/10.1111/lasr.12681> accessed 20 July 2026
7. Busuioc M, 'Accountable Artificial Intelligence: Holding Algorithms to Account' (2021) 81(5) Public Administration Review 825 <https://doi.org/10.1111/puar.13293> accessed 20 July 2026
8. Calo R and Citron DK, 'The Automated Administrative State: A Crisis of Legitimacy' (2021) 70(4) Emory Law Journal 797 <https://scholarlycommons.law.emory.edu/elj/vol70/iss4/1> accessed 20 July 2026
9. Carney T, 'Robo-Debt Illegality: The Seven Veils of Failed Guarantees of the Rule of Law?' (2019) 44(1) Alternative Law Journal 4 <https://doi.org/10.1177/1037969X18815913> accessed 20 July 2026
10. Clapham N, 'The Authorisation of Surveillance: A Separation of Power?' (*UK Constitutional Law Association Blog*, 25 June 2015) <https://ukconstitutionallaw.org/2015/06/25/nicholas-clapham-the-authorisation-of-surveillance-a-separation-of-power/> accessed 20 July 2026
11. Cobbe J, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making' (2019) 39(4) Legal Studies 636 <https://doi.org/10.1017/lst.2019.9> accessed 20 July 2026
12. Eisenberger I, 'Technology's Self-Governance' in Brownsword R and DiMatteo LA (eds), *The Cambridge Handbook of the Governance of Technology* (CUP 2026) 22 <https://doi.org/10.1017/9781009522519.004> accessed 20 July 2026

13. Enqvist L and Naarttijärvi M, 'Discretion, Automation, and Proportionality' in Suksi M (ed), *The Rule of Law and Automated Decision-Making* (Springer 2023) 147 <https://doi.org/10.1007/978-3-031-30142-1_7> accessed 20 July 2026

14. Ghappour A, 'Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web' (2017) 69(4) Stanford Law Review 1075

15. Graziani C, 'Technosecuritisation: Digital Technologies and the Securitisation of EU Migration Law' (2026) 28(1) European Journal of Migration and Law 34 <https://doi.org/10.1163/15718166-12340215> accessed 20 July 2026

16. Grzelak A, 'Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11' (2016) 22(3) European Public Law 475 <https://doi.org/10.54648/euro2016030> accessed 20 July 2026

17. Megiddo T, 'Online Activism, Digital Domination, and the Rule of Trolls' (2020) 58(2) Columbia Journal of Transnational Law 394 <https://dx.doi.org/10.2139/ssrn.3459983> accessed 20 July 2026

18. Möllers C, *The Three Branches: A Comparative Model of Separation of Powers* (OUP 2013) <https://doi.org/10.1093/acprof:oso/9780199602117.002.0008> accessed 20 July 2026

19. Montesquieu, *The Spirit of the Laws* (AM Cohler, BC Miller, and HS Stone eds, CUP 1989)

20. Pettit P, *Republicanism: A Theory of Freedom and Government* (OUP 1997) <https://doi.org/10.1093/0198296428.001.0001> accessed 20 July 2026

21. Porcedda MG, 'Automated Analysis in the AFSJ and Digital Single Market Monitoring: An Effaced Nexus' in Kosta E and Kamara I (eds), *Data Retention in Europe and Beyond* (OUP 2025) 423 <https://doi.org/10.1093/9780191998980.003.0028> accessed 20 July 2026

22. Rabinovych M, 'EU Enlargement Policy Goes East: Historical and Comparative Takes on the EU's Rule of Law Conditionality vis-à-vis Ukraine' (2024) 16 Hague Journal on the Rule of Law 715 <https://doi.org/10.1007/s40803-024-00223-6> accessed 20 July 2026

23. Rachovitsa A and Johann N, 'The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case' (2022) 22(2) Human Rights Law Review 1 <https://doi.org/10.1093/hrlr/ngac010> accessed 20 July 2026

24. Rojszczak M, 'EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses' (2021) 29(3-4) European Journal of Crime, Criminal Law and Criminal Justice 290 <https://doi.org/10.1163/15718174-bja10027> accessed 20 July 2026

25. Rojszczak M, 'Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland' (2021) 17(1) Democracy and Security 1 <https://doi.org/10.1080/17419166.2020.1841367> accessed 20 July 2026

26. Sadurski W, *Poland's Constitutional Breakdown* (OUP 2019)

27. Solove DJ, *Understanding Privacy* (Harvard UP 2008) <https://ssrn.com/abstract=1127888> accessed 20 July 2026

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

28. Szwajdler P, 'Automated Judicial Decision-Making Systems and New Legal Principles' [2026] Constitutional Political Economy 1 <https://doi.org/10.1007/s10602-025-09490-3> accessed 20 July 2026

29. Vile MJC, *Constitutionalism and the Separation of Powers* (2nd edn, Liberty Fund 1998)

30. Webber F, 'Impunity Entrenched: The Erosion of Human Rights in the UK' (2022) 63(4) Race & Class 56 <https://doi.org/10.1177/03063968221083193> accessed 20 July 2026

31. Zalnieriute M, Moses LB and Williams G, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82(3) Modern Law Review 425 <https://doi.org/10.1111/1468-2230.12412> accessed 20 July 2026

32. Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019)

AUTHORS' INFORMATION

Adem Ersin Bayra*
PhD, Associate Professor, Faculty of Law, Istanbul Medipol University, Istanbul, Türkiye
ersin.bayra@gmail.com
https://orcid.org/0000-0002-3391-6707
Corresponding author; responsible for Conceptualisation, Methodology, Investigation, Writing – original draft, Writing – review & editing.

Nihat Bulut
PhD, Professor, Faculty of Law, Istanbul Medipol University, Istanbul, Türkiye
nihat.bulut@medipol.edu.tr
https://orcid.org/0000-0002-7318-0466
Co-author; responsible for Conceptualisation, Supervision, Validation, Writing – review & editing.

Competing interests: The authors declare no competing interests.

Disclaimer: The authors declare that their opinions and views expressed in this manuscript are free of any organisational impact.

FUNDING STATEMENT

This research received no external funding. The authors' university funded the APC for this publication, in accordance with the AJEE Charges Policy.

RIGHTS AND PERMISSIONS

Copyright: © 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

EDITORS

Managing Editor – Mag. Yuliia Hartman. **English Editor** – Robert Reddin.
Ukrainian Editor – Liliia Hartman.

ABOUT THIS ARTICLE

Cite this article
Bayra AE and Bulut N, 'Who Authorises Surveillance? Coercive Digital Surveillance, the Rule of Law, and Access to Judicial Oversight: A Central and Eastern European Perspective' (2026) 9(4) Access to Justice in Eastern Europe 485-514 <https://doi.org/10.33327/AJEE-18-9.4-a0002024>

DOI: https://doi.org/10.33327/AJEE-18-9.4-a0002024

Summary: 1. Introduction. – 2. Aims, Research Questions and Methodology. – 3. A Shift in Framework: From Privacy to Authorisation. – 4. The Four Hinges of Authorisation. – *4.1. Legislative Reserve. – 4.2. Independent Prior Authorisation. – 4.3. Ex Post Oversight and Effective Remedies: The Collapse of Access to Justice. – 4.4. The Role of Private Actors.* – 5. Comparative Application: Central and Eastern Europe and the EU Axis. – 6. Authorisation Architecture: A Graduated Standard. – 7. Objections and Limitations. – 8. Conclusion.

***Keywords*:** *Digital Surveillance; Separation of Powers; Rule of Law; Access to Justice; Automated Decision-Making; Pegasus; Central and Eastern Europe.*

DETAILS FOR PUBLICATION

Date of submission: 26 Jul 2026
Date of acceptance: 18 Sep 2026
Online First Publication: 23 Oct 2026
Last Publication: 03 Nov 2026
Was the manuscript fast-tracked? – No
Number of reviewer reports submitted in the first round: 2 reports
Number of revision rounds: 1 round with minor revisions

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Technical tools used in the editorial process

Plagiarism checks - Turnitin from iThenticate
https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review
https://scholasticahq.com/law-reviews
Paperpal for Academic Editing & Proofreading
https://paperpal.com/

AI DISCLOSURE STATEMENT

This article was prepared with the assistance of AI tools. Specifically, Claude (Anthropic) was used for language editing and citation-format checking during the preparation of the English text (May to July 2026). The authors confirm that they generated all content, arguments, and conclusions independently and that they remain solely responsible. No AI tool was used for generating original research findings or analysis.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ХТО НАДАЄ ДОЗВІЛ НА СПОСТЕРЕЖЕННЯ? ПРИМУСОВЕ ЦИФРОВЕ СПОСТЕРЕЖЕННЯ, ВЕРХОВЕНСТВО ПРАВА ТА ДОСТУП ДО СУДОВОГО НАГЛЯДУ: ДОСВІД КРАЇН ЦЕНТРАЛЬНОЇ ТА СХІДНОЇ ЄВРОПИ

Адем Ерсін Байра* та Ніхат Булут

АНОТАЦІЯ

Передумови. *Дискусії щодо цифрового спостереження переважно зосереджені на захисті права на приватність і персональних даних. Проте фундаментальна конституційно-правова проблема примусового цифрового спостереження полягає не стільки в серйозності втручання, скільки в тому, хто саме надає дозвіл на його здійснення та яким механізмам контролю воно підлягає. Іншими словами, йдеться насамперед про поділ влади та доступ до правосуддя.*

Методи. *Дослідження ґрунтується на порівняльно-доктринальному підході. У ньому проаналізовано чотири юрисдикції — Польщу, Угорщину, Україну та Сполучене Королівство, відібрані методом цільової вибірки. Джерельну базу становлять матеріали розслідування Європейського парламенту в межах діяльності комітету PEGA, судова практика Європейського суду з прав людини (ЄСПЛ) і Суду справедливості Європейського Союзу (СЄС), а також звіти Європейської комісії.*

Результати та висновки. *Поступове перенесення повноважень щодо надання дозволів на спостереження від законодавчої влади до виконавчої, а надалі — до нижчих ланок управління та дедалі частіше до приватних суб'єктів, зумовило необхідність дослідження системи санкціонування крізь призму чотирьох ключових елементів: вимоги законодавчого регулювання (legislative reserve), незалежного попереднього санкціонування, ефективного подальшого (ex post) контролю та запобіжників від надмірного делегування повноважень. У дослідженні продемонстровано, як цифрове спостереження створює системні виклики для кожного із цих елементів та як ці проблеми проявляються в досліджуваних юрисдикціях. Науковий внесок дослідження полягає в переосмисленні цифрового спостереження насамперед як проблеми розподілу повноважень, у визначенні чотирьох ключових елементів системи санкціонування та розробленні кумулятивного тесту належності санкціонування, вимоги якого диференціюються залежно від інтенсивності втручання. У межах цієї концепції доступ до правосуддя є необхідною передумовою легітимності, а запропонований критерій може застосовуватися в різних типах політичних режимів. Порівняльний аналіз підтверджує цей висновок: у Польщі та Угорщині всі чотири елементи одночасно демонструють системні недоліки; в Україні три з них перебувають у процесі відновлення та перебудови згідно з умовами вступу до ЄС; у Сполученому Королівстві посилення лише одного з елементів виявилося недостатнім для компенсації недоліків інших елементів системи. Дослідження доводить, що навіть найретельніша перевірка пропорційності втручання не може усунути недоліків, допущених на етапі надання дозволу.*

Ключові слова: *цифрове спостереження; поділ влади; верховенство права; доступ до правосуддя; автоматизоване ухвалення рішень; Pegasus; Центральна та Східна Європа.*

ABSTRACT IN TURKISH*

Araştırma Makalesi

GÖZETİMİ KİM YETKİLENDİRİR? ZORLAYICI DİJİTAL GÖZETİM, HUKUK DEVLETİ VE YARGISAL DENETİME ERİŞİM — ORTA VE DOĞU AVRUPA'DAN BİR BAKIŞ

Adem Ersin Bayra*, Nihat Bulut

ÖZET

Arka Plan: *Dijital gözetime ilişkin tartışmalar büyük ölçüde mahremiyet ve kişisel verilerin korunması ekseninde yürütülmektedir. Oysa zorlayıcı dijital gözetimin asıl anayasal sorunu, müdahalenin ağırlığından ziyade bu müdahaleyi kimin yetkilendirdiği ve müdahalenin hangi denetime tabi kılındığıdır. Yani mesele esasen bir kuvvetler ayrılığı ve adalete erişim meselesidir.*

* The publication metadata in Turkish is presented as submitted by the authors.

© 2026 Adem Ersin Bayra and Nihat Bulut. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Metodoloji: *Çalışma karşılaştırmalı doktriner bir yöntemle yürütülmektedir. Amaçlı örnekleme ile seçilmiş dört ülke (Polonya, Macaristan, Ukrayna ve Birleşik Krallık) Avrupa Parlamentosu PEGA Soruşturması, Avrupa İnsan Hakları Mahkemesi ile Avrupa Birliği Adalet Divanı içtihadı ve Avrupa Komisyonu raporları üzerinden çözümlenmektedir.*

Bulgular ve Sonuçlar: *Gözetime izin verme yetkisinin yasamadan yürütmeye, oradan idarenin alt birimlerine ve giderek özel aktörlere kayışı, yetkilendirme mimarisinin dört menteşe üzerinden ele alınmasını gerektirmiştir. Bunlar yasama saklı alanı, bağımsız ön onay, uygulama sonrası etkili denetim ve yetki devri güvenceleridir. Çalışmada dijital gözetimin her menteşeyi nasıl ayrı ayrı zorladığı ve örneklemde nasıl somutlaştığı ortaya konulmaktadır. Çalışmanın katkısı, dijital gözetimi öncelikle bir yetki tahsisi meselesi olarak yeniden çerçevelemek, yetkilendirme mimarisinin dört menteşesini adlandırmak ve müdahalenin yoğunluğuna göre kademelenen kümülatif bir yetkilendirme ölçütü önermektir. Bu çerçevede adalete erişim bir meşruiyet önkoşuluna dönüşmekte, ölçüt ise farklı rejim tipleri arasında taşınabilir hâle gelmektedir. Örnek olaylar da bunu doğrulamaktadır. Polonya ve Macaristan'da dört menteşe aynı anda işlevini yitirmekte, Ukrayna'da bunlardan üçü AB katılım koşulluluğu altında yeniden kurulmakta, Birleşik Krallık'ta ise tek bir menteşenin güçlendirilmesi diğerlerindeki zayıflığı telafi etmeye yetmemektedir. Karşılaştırma, ölçülülük denetimi ne kadar titizlikle yapılırsa yapılsın yetkilendirme aşamasındaki bir kusurun giderilemeyeceğini göstermektedir.*

Anahtar Kelimeler: *adalete erişim; dijital gözetim; hukuk devleti; kuvvetler ayrılığı; otomatik karar alma; Orta ve Doğu Avrupa; Pegasus.*