UDC 342.98:343.982.34
DOI: 10.63341/naia-herald/2.2026.47

ISSN 2410-3594
E-ISSN 2786-7382

Biometric registration of public servants: Between state security and the right to privacy

Mykola Komissarov*
PhD in Law, Associate Professor
Centre for Internal Special-Purpose Security "Hard", National Guard of Ukraine
03151, 9A Svyatoslav Khorobryho Str., Kyiv, Ukraine
https://orcid.org/0000-0001-6828-7974

Natalia Komissarova
PhD in Law, Associate Professor
Kyiv Institute of the National Guard of Ukraine
03180, 7 Oborony Kyiva Str., Kyiv, Ukraine
https://orcid.org/0000-0001-6895-6891

■ **Abstract.** This article examines the legal regulation of mandatory fingerprinting of civil servants as a mechanism for identity verification, integrity assurance, and security in public administration. Using comparative legal and formal legal methods, legislation of Ukraine, European Union member states, and the United States is analysed with respect to the collection and processing of fingerprint data of persons holding or applying for public service positions. The practice of the European Court of Human Rights in "S. and Marper v. the United Kingdom" and "Gaughran v. the United Kingdom", and the Court of Justice of the European Union in Case No. C-371/24 "Comdribus", are systematised. The principal results are as follows. Ukraine has no statutory provision for fingerprinting upon entry to public service – for civilian servants, police officers, or military personnel alike – constituting a structural vulnerability of the public administration integrity system. The approach that the General Data Protection Regulation prohibits such registration is shown to be doctrinally erroneous: Article 9(2)(g) General Data Protection Regulation expressly permits processing of biometric data on grounds of substantial public interest where a proper statutory basis exists. A differentiated model for introducing fingerprinting compatible with European Court of Human Rights, Court of Justice of European Union, and General Data Protection Regulation standards is substantiated. The wartime dimension – identification of fallen military personnel – is identified and its normative resolution proposed. The adoption of a Law of Ukraine "On Biometric Registration" with a differentiated approach to position categories, clear data protection guarantees, and phased implementation is the primary legislative step required

■ **Keywords**: biometric registration; personal data protection; civil service integrity; right to privacy; identification of the fallen

■ Introduction

The question of whether civil servants should be subject to mandatory fingerprint registration upon entry to public service has acquired particular normative urgency in Ukraine in 2026 for reasons that are simultaneously legal, institutional, and humanitarian. Ukraine's ongoing accession to the European Union (EU) requires demonstrated compliance with supranational data protection standards that directly govern the permissibility of biometric registration by public authorities – a legislative task that remains unaddressed at the statutory level. Concurrently, conditions of full-scale armed conflict have exposed with

■ **Suggested Citation:**
Komissarov, M., & Komissarova, N. (2026). Biometric registration of public servants: Between state security and the right to privacy. *Scientific Journal of the National Academy of Internal Affairs,* 31(2), 47-58. doi: 10.63341/naia-herald/2.2026.47.

■ *Corresponding author (*nikkorov@ukr.net*)

■ Received: 16.01.2026; Revised: 14.04.2026; Accepted: 26.05.2026; Published: 01.06.2026

unprecedented clarity the practical consequences of the absence of a pre-existing biometric record for public servants and military personnel: the inability to rapidly identify those missing or killed in the line of duty. From a theoretical standpoint, the subject reveals a structural blind spot in Ukrainian administrative law: the administrative-law dimension of biometric registration has received virtually no doctrinal treatment, despite its direct implications for civil service integrity, access to classified information, and the protection of fundamental rights. Addressing this gap is therefore not merely a matter of legislative technique but a condition of Ukraine's capacity to meet its European integration commitments whilst simultaneously safeguarding the rights of persons subject to biometric data collection by the state.

The most recent scholarship has addressed specific dimensions of this problem from several directions. S. Knyzhenko & O. Sharaban (2023) examined the legal regulation of the fingerprint registration system maintained by the Ministry of Internal Affairs of Ukraine, concluding that the existing normative framework is marked by significant internal contradictions and leaves fundamental questions of data retention, access, and oversight unresolved at the statutory level. Y. Orlov & N.O. Pribytkova (2022) analysed the impact of armed conflict on criminal law policy in Ukraine, establishing that the conditions of full-scale war create a heightened institutional demand for reliable biometric identification procedures that existing legislation is structurally unprepared to meet. D.J. Solove & P.M. Schwartz (2019) examined contemporary privacy law frameworks across multiple jurisdictions, demonstrating that effective statutory regulation of biometric data must incorporate purpose-limitation, proportionality, and rights-of-access guarantees as non-derogable minimum standards. A.K. Jain *et al.* (2011) established the foundational technical and normative parameters of contemporary biometric recognition systems, demonstrating that fingerprint identification achieves operational reliability only when embedded within a comprehensive identity management infrastructure governed by transparent legal rules. D. Lyon (2009) analysed the social and political dimensions of state-mandated biometric identification schemes, concluding that their democratic legitimacy is contingent upon robust accountability mechanisms and clearly delimited statutory purposes. B. Loomis & K. Bowerman (2025) studied the operational use of biometric intelligence in grey zone conflicts within the NATO framework, concluding that the institutional reliance on biometric data in allied security architectures generates direct normative expectations for member states to maintain pre-existing biometric records of their military personnel. The Media Initiative for Human Rights (2024) investigated the identification of persons missing as a result of the armed conflict, establishing that the absence of pre-existing biometric records of military personnel extends the identification timeline to fourteen months in DNA-based procedures – a delay that would be substantially reduced by systematic prior fingerprint registration. ZMINA (2025) documented the search and identification practices applied to persons missing during the war, revealing that existing institutional capacities are critically insufficient and that biometric data infrastructure represents the primary systemic gap requiring legislative remedy. Notwithstanding this growing body of literature, a comprehensive administrative-law study of the legal vacuum in the sphere of fingerprinting public servants in Ukraine – integrating European Court of Human Rights (ECtHR) and Court of Justice of European Union (CJEU) standards with the wartime identification dimension – has not been undertaken.

The aim of this study was, on the basis of a comparative legal analysis of the legislation and judicial practice of Ukraine, the EU, and the USA, to determine the state of legal regulation of fingerprinting of persons holding positions in public service and to formulate scientifically grounded proposals for the improvement of national legislation. To achieve this aim, three interrelated objectives were pursued: (1) to establish the theoretical and legal foundations of fingerprinting in the public administration system, including the legal status of fingerprint data as a category of personal data; (2) to conduct a comparative legal analysis of the relevant legislation and judicial practice of the USA, EU member states, and post-Soviet states, with particular attention to the standards established by the ECtHR and the CJEU; (3) to identify the systemic gaps in the national legal framework and to substantiate a model of legislative regulation compatible with international human rights standards. The scientific novelty of the research consists of the first comprehensive characterisation of the legal vacuum in the sphere of fingerprint registration of public servants in Ukraine, the justification of a differentiated model for the introduction of fingerprinting consistent with ECtHR, CJEU, and GDPR standards, and the identification of the wartime identification dimension as a specific normative problem requiring legislative resolution.

Literature Review

The scholarly literature on biometric registration and fingerprinting in the public law context may be structured around three principal streams: criminalistic and forensic studies, data-protection and privacy scholarship, and public administration and security research. The following review focuses on foundational works that established the analytical parameters of the field, whilst the most recent

contributions (2021 onwards) have been incorporated into the Introduction above.

Within the first stream, V. Zakharov & V. Rudeshko (2015) produced a foundational monograph on biometric technologies and their application by law enforcement agencies, examining dactyloscopy as a core identification instrument from both technical and legal perspectives and concluding that the legal regulation of biometric identification in Ukraine required substantial modernisation. H. Bidniak (2017) analysed the normative-legal regulation of fingerprinting of persons in Ukraine, identifying significant statutory lacunae and arguing that the absence of a comprehensive legislative framework created risks of arbitrary application of existing subordinate acts by executive authorities. Together, these works established that the criminalistic dimension of dactyloscopy in Ukraine was substantively regulated, whilst the administrative dimension – specifically, the fingerprinting of public servants – remained entirely unaddressed.

The data-protection and privacy stream has produced the most theoretically sophisticated treatment of the subject. E.J. Kindt (2013) conducted a landmark comparative legal analysis of biometric applications across multiple jurisdictions, establishing that biometric data possess a uniquely sensitive character – owing to their immutability and potential link to criminal registers – and concluding that national legislative frameworks must incorporate proportionality, purpose-limitation, and data-minimisation principles as minimum standards. P. De Hert & A. Sprokkereef (2008) examined the tension between the deployment of biometric data by public authorities and the requirements of EU data protection law, arguing that the emerging "biometric state" tendency must be constrained by the necessity and proportionality principles enshrined in both the ECHR and the EU fundamental rights. A.F. Westin (2003) explored the social and political dimensions of informational privacy, demonstrating that the level of public trust in state biometric practices is contingent on the strength of procedural guarantees and the degree of democratic oversight. E. Mordini & D. Tzovaras (2012) edited a comprehensive collection examining the ethical, legal, and social context of second-generation biometrics, concluding that emerging biometric technologies demand a regulatory response that is adaptive, rights-based, and sensitive to the distinction between public-order and private-sector applications.

K.D. Haggerty & R.V. Ericson (2000) developed the concept of the "surveillant assemblage," arguing that contemporary surveillance systems increasingly combine disparate forms of personal data into integrated digital identities, thereby transforming traditional understandings of privacy and state monitoring. Their analysis is directly relevant to biometric registration of public servants because it demonstrates that biometric identifiers, once incorporated into interconnected state databases, may facilitate pervasive forms of administrative surveillance that require strict legal limitations, proportionality safeguards, and democratic oversight. C.J. Bennett (2010) examined the emergence of transnational privacy advocacy networks resisting the expansion of surveillance technologies, including biometric identification systems, data profiling, and state monitoring practices, arguing that privacy protection increasingly depends on civil-society mobilisation and democratic oversight rather than solely on formal legal safeguards.

J. Ashbourn (2014) substantially expanded the discussion of biometrics beyond purely technical and forensic considerations by examining biometric identity management within the broader contexts of cloud computing, mobile technologies, and transnational data infrastructures. The author demonstrated that the increasing integration of biometric systems into public administration and digital governance creates heightened risks for informational privacy, particularly where biometric identifiers are processed across institutional and geographic boundaries without sufficiently robust safeguards, oversight mechanisms, and purpose limitations. In the context of biometric registration of public servants, J. Ashbourn (2014) work is especially significant because it frames biometrics not merely as a security instrument, but as a component of pervasive identity management that requires a careful balance between state security interests and the protection of individual privacy rights. R. Brownsword & M. Goodwin (2012) examined the interaction between emerging technologies, regulatory systems, and fundamental rights in the twenty-first century, arguing that modern legal frameworks increasingly struggle to balance technological efficiency with the preservation of individual autonomy and privacy. In the context of biometric registration of public servants, the work is significant because it conceptualises biometric surveillance and identity management as part of a broader transformation toward technologically mediated governance, where security-oriented state practices must remain constrained by proportionality, accountability, and human-rights protections.

The third stream – addressing institutional and security dimensions – has generated insights of direct relevance to the present study. M. Zwanenburg (2012) examined the intersection of biometric data collection and international humanitarian law, establishing that the collection of biometric information from persons in the context of armed conflict raises specific legal obligations under the Geneva Conventions and customary international humanitarian law, with particular implications for the identification of casualties. L. Zouhar & M.G. Bartoszewicz (2022) demonstrated, in a different but

methodologically instructive context, that the formal legal regime governing the classification of objects – rather than their physical properties – determines which instruments are actually encountered in practice; this insight is directly applicable to the analysis of biometric registration regimes, where the formal legal status assigned to fingerprint data determines the scope of rights and obligations of the persons whose data are collected.

The foregoing review reveals two significant gaps in the existing literature. First, whilst the international and comparative scholarship has extensively theorised the conditions for lawful biometric data collection in general terms, the specific administrative-law question of the fingerprinting of public servants – as distinct from criminal registration – has not been subjected to systematic doctrinal analysis in the Ukrainian context. Second, the wartime dimension of the problem – namely, the use of prior fingerprint registration records for the identification of fallen military personnel – represents an entirely novel normative question that the existing literature has not addressed from a legislative-design perspective. The present study seeks to fill both gaps.

■ Materials and Methods

The methodological basis of the research comprised a set of scientific methods selected in accordance with the nature of its object and subject. The comparative legal method was employed to juxtapose the legal systems of different states according to uniform criteria – specifically, the statutory basis for fingerprint registration, the categories of persons subject to registration, the conditions for data storage and deletion, and the available oversight mechanisms – thereby enabling the construction of the comparative table presented in the Results section. The formal legal method was applied in the analysis of normative legal acts and judicial decisions, including the Law of Ukraine "On Civil Service"[1], the Law of Ukraine "On the National Police"[2], Resolution No. 1214 of the Cabinet of Ministers of Ukraine[3], Article 9(2)(g) of the GDPR[4], the Grand Chamber judgment of the ECtHR in S. and Marper v. the United Kingdom[5], the judgment in Gaughran v. the United Kingdom[6], and the CJEU ruling in Case No. C-371/24[7]. The systemic method was used to examine the interconnections between the norms on personal data protection and the norms on public service, making it possible to identify the structural nature of the existing regulatory gap and to trace the consequences of that gap across different branches of national law.

The empirical basis of the research comprised: primary legislative and regulatory sources of Ukraine, the USA, the EU and its member states, Moldova, and Kazakhstan; the case law of the ECtHR and the CJEU; official statistics of the Unified Register of Persons Missing under Special Circumstances; and analytical reports of Ukrainian and international human rights organisations (Media Initiative for Human Rights, 2024; ZMINA, 2025). The study covered the period from 2003 (adoption of the Moldovan Law on State Dactyloscopic Registration) to 2026 (CJEU ruling in Case No. C-371/24[8]). Each normative source was assessed against the four-criterion compliance framework (lawful basis, legitimate aim, proportionality, and effective oversight) derived from the synthesis of ECtHR and CJEU case law, thereby ensuring methodological consistency across jurisdictions. The choice of comparative jurisdictions – the USA, EU member states (with a focus on the Netherlands), Moldova, and Kazakhstan – was determined by their representativeness of different approaches to fingerprint registration of public servants: a comprehensive mandatory model (USA), a differentiated model within the GDPR framework (EU), and post-Soviet legislative codification (Moldova, Kazakhstan)[9].

■ Results

Fingerprinting in the public administration system: Theoretical foundations. In the scholarly literature, a well-established distinction is drawn between fingerprinting according to its sphere of application: criminal registration (within criminal

[1] Law of Ukraine No. 889-VIII "On Civil Service". (2015, December). Retrieved from https://zakon.rada.gov.ua/laws/show/889-19.
[2] Law of Ukraine No. 580-VIII "On the National Police". (2015, July). Retrieved from https://zakon.rada.gov.ua/laws/show/580-19.
[3] Resolution of the Cabinet of Ministers of Ukraine No. 1214 "On the Approval of the Procedure for Implementing the Experimental Project on Identification of the Remains of Those Killed as a Result of the Armed Aggression of the Russian Federation Against Ukraine by Means of Biometric Data". (2025, September). Retrieved from https://legal100.org.ua/yak-teper-budut-identyfikovuvaty-zagyblyh-vijskovyh-postanova-km-ukrayiny-%E2%84%96-1214/.
[4] General Data Protection Regulation. (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[5] Judgment of the European Court of Human Rights in the Case No. 30562/04 and 30566/04 "S. and Marper v. the United Kingdom". (2008, December). Retrieved from https://hudoc.echr.coe.int/fre?i=001-90051.
[6] Judgment of the European Court of Human Rights in the Case No. 45245/15 "Gaughran v. the United Kingdom". (2020, February). Retrieved from https://hudoc.echr.coe.int/fre?i=001-200817.
[7] Judgment of the Court of Justice of the European Union in Case No. C-371/24 "Comdribus". (2026, March). Retrieved from https://curia.europa.eu/site/upload/docs/application/pdf/2026-03/cp260039en.pdf.
[8] Ibidem, 2026.
[9] Judgment of the European Court of Human Rights in the Case No. 30562/04 and 30566/04 "S. and Marper v. the United Kingdom". (2008, December). Retrieved from https://hudoc.echr.coe.int/fre?i=001-90051.

proceedings) and administrative registration (outside criminal justice, in particular for the purposes of verifying persons upon entry to service, access control, and similar purposes). As noted by V. Zakharov & V. Rudeshko (2015), dactyloscopy is one of the fundamental instruments for the identification of a person by biometric data and stands at the intersection of forensic science, administrative law, and information law.

In the context of public service, fingerprinting performs three independent functions. The identification function consists in establishing the identity of a person and making it impossible to use forged documents. The preventive function is directed towards preventing the appointment to positions of persons with a criminal past, concealed connections, or a dual identity. The operational-security function provides access control to protected facilities and classified materials. This classification is important for distinguishing between the legal regimes governing the collection and use of the data obtained (Bidniak, 2017). From the standpoint of public administration theory, the introduction of fingerprinting fits within the concept of the "biometric state" – a state that systematically uses citizens' biological characteristics for administrative and security purposes. National Research Council (2010) draw attention to the fact that this tendency requires balancing against the principle of minimality of interference with private life and cannot be realised outside clear legislative frameworks.

Pursuant to the GDPR[1], biometric data that are subject to specific technical processing and enable the unambiguous identification of a natural person constitute a "special category" of personal data, the processing of which is in principle prohibited (Art. 9). The particular legal nature of fingerprint data is conditioned by their immutability – a papillary pattern cannot be "revoked" or replaced, unlike a password or document number – as well as by their potential link to criminal registers and the irreversibility of the consequences of their disclosure (Koops & Leenes, 2013). These characteristics distinguish fingerprint data from other categories of personal information and impose a correspondingly elevated standard of justification on any public authority seeking to collect and retain them.

The foregoing theoretical analysis warrants the following interim conclusions. First, fingerprinting in the context of public administration constitutes a distinct form of administrative biometric registration, functionally separate from criminal dactyloscopy: it serves identification, preventive, and operational-security functions and is oriented not toward establishing the facts of an offence, but toward ensuring the integrity and reliability of the public service. Second, fingerprint data fall within the category of biometric personal data subject to heightened protection under Article 9 GDPR, owing to their immutability, their potential link to criminal registers, and the irreversibility of harm in the event of unauthorised disclosure. Third, the tension identified by P. De Hert & A. Sprokkereef (2008) between biometric state practices and the principle of minimal interference with private life does not preclude administrative fingerprinting per se, but requires that any such measure be grounded in a clear statutory basis, pursue a legitimate aim, and satisfy the test of proportionality. These theoretical parameters define the analytical framework applied in the comparative assessment that follows.

International experience: A comparative legal analysis. The foundational legal reference point in the sphere of the protection of fingerprint data is the practice of ECtHR. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms[2] guarantees the right to respect for private and family life, which encompasses the protection of personal data, including biometric data. The key precedent is the Grand Chamber judgment in S. and Marper v. the United Kingdom[3]. The Court unanimously found a violation of Art. 8 of the Convention in connection with the indefinite retention of fingerprints and DNA profiles of persons subsequently acquitted. In Gaughran v. the United Kingdom[4] the ECtHR extended this position to persons with spent convictions, finding that the indefinite retention of their biometric data – in the absence of a differentiated approach that took account of the gravity of the offence and the genuine necessity of prolonged retention – was incompatible with Art. 8 of the Convention[5].

The ECtHR practice was further developed by the Court of Justice of the European Union in Case C-371/24[6]. Interpreting Art. 10 of Directive

[1] General Data Protection Regulation. (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[2] Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://www.echr.coe.int/documents/d/echr/convention_ENG.
[3] Judgment of the European Court of Human Rights in the Case No. 30562/04 and 30566/04 "S. and Marper v. the United Kingdom". (2008, December). Retrieved from https://hudoc.echr.coe.int/fre?i=001-90051.
[4] Judgment of the European Court of Human Rights in the Case No. 45245/15 "Gaughran v. the United Kingdom". (2020, February). Retrieved from https://hudoc.echr.coe.int/fre?i=001-200817.
[5] Ibidem, 2020.
[6] Judgment of the Court of Justice of the European Union in Case No. C-371/24 "Comdribus". (2026, March). Retrieved from https://curia.europa.eu/site/upload/docs/application/pdf/2026-03/cp260039en.pdf.

No. 2016/680/EU[1], the CJEU held that the collection of biometric data by competent authorities is permissible exclusively on condition of strict necessity and with a mandatory individual justification for each decision. National legislation making such collection systematic – without an individual assessment of strict necessity – is contrary to EU law.

A synthesis of ECtHR and CJEU practice makes it possible to identify four key principles: (1) a lawful basis in law; (2) a strictly necessary and legitimate aim; (3) proportionality; and (4) effective guarantees and review mechanisms. These principles constitute the minimum standard for any fingerprint registration regime for public servants. The United States represents an example of a state with a developed system of fingerprint checks for persons in public service. Every person entering federal civil service is obliged to provide fingerprints for a criminal background check through the FBI's Next Generation Identification (NGI) database (Federal Bureau of Investigation, 2023). The level of screening is differentiated by risk category (U.S. Department of the Interior, 2023). A system-forming element of the American model is the "Rap Back" continuous monitoring mechanism, under which the FBI promptly notifies the relevant authorities of new criminal records concerning already verified employees (Federal Bureau of Investigation, 2023). The American model thus combines mandatory biometric registration upon entry with continuous dynamic monitoring throughout the period of service.

In EU member states, approaches to the fingerprinting of public servants differ, but all are realised within the GDPR framework. Article 9(2)(g) GDPR provides for an exception to the general prohibition on the processing of biometric data in cases where such processing is necessary for reasons of substantial public interest on the basis of the legislation of a member state. The enforcement practice of the Netherlands is illustrative: the Dutch Data Protection Authority imposed on an employer a fine of EUR 725,000 for the mandatory scanning of employees' fingerprints, finding that the employer had failed to demonstrate either the existence of explicit consent or the impossibility of applying less invasive means of identification (datenshutz, 2020). This precedent illustrates the principled approach: mandatory fingerprint registration requires an unambiguous legislative authorisation and proof of proportionality.

Among post-Soviet states, Moldova adopted a separate Law on State Dactyloscopic Registration[2], which systematically defines the list of persons subject to mandatory fingerprinting, the principles of legality and confidentiality, and the guarantees for data protection. Kazakhstan adopted the Law on Dactyloscopic and Genomic Registration in 2016[3], providing for mandatory fingerprinting for persons entering service in law enforcement agencies. These examples demonstrate that even in states with transitional legal systems, special legislative regulation at the statutory level is recognised as necessary.

In the sphere of the armed forces, the American experience is particularly instructive: the U.S. Army introduced mandatory fingerprinting of recruits as early as 1905. Owing to preserved fingerprint records, all 45,952 Americans killed in Vietnam were identified (U.S. Office of Justice Programs, 1982). The current U.S. legislation[4] enshrines the mandatory collection of fingerprints upon entry into military service. In October 2022, the U.S. Secretary of the Army approved the first Army Biometrics Directive (U.S. Army, 2022). Within the NATO framework, the Automated Biometric Identification System (ABIS/NABIS) operates, providing for the exchange of biometric data between allies during joint operations (Loomis & Bowerman, 2025).

The comparative analysis of international practice yields the following interim conclusions. First, a synthesis of ECtHR and CJEU case law establishes four minimum quality requirements for any fingerprint registration regime: a lawful basis in statute, a strictly necessary and legitimate aim, proportionality, and effective oversight and review mechanisms. These requirements, whilst they set a high threshold, do not constitute an absolute prohibition on administrative fingerprinting of public servants. Second, the United States model – combining mandatory entry-level registration with continuous Rap Back monitoring – demonstrates the operational feasibility of comprehensive biometric verification of the public service workforce within a rule-of-law framework. Third, EU member states pursue a differentiated approach calibrated to the sensitivity of the position, utilising the public-interest exception under Article 9(2)

[1] Directive No. 2016/680 EU "On the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng.

[2] Law of the Republic of Moldova No. 1549-XV "On State Dactyloscopic Registration". (2003, February). Retrieved from https://www.ecoi.net/en/file/local/1027471/1504_1217232004_law-of-the-republic-of-moldova-on-state-dactyloscopic-registration.pdf.

[3] Law of the Republic of Kazakhstan No. 40-IV "On Dactyloscopic and Genomic Registration". (2016, December). Retrieved from https://adilet.zan.kz/eng/docs/Z1600000040.

[4] 8 U.S. Code § 1440f "Fingerprints and Other Biometric Information for Members of the United States Armed Forces. Legal Information Institute". (2008, June). Retrieved from https://www.law.cornell.edu/uscode/text/8/1440f.

(g) GDPR; the Dutch enforcement practice confirms that mandatory registration requires unambiguous legislative authorisation and proof of proportionality in each case. Fourth, the post-Soviet experience of Moldova (2003) and Kazakhstan (2016) illustrates that statutory codification of biometric registration regimes is achievable even in transitional legal systems. Fifth, and most significantly for the purposes of this article, none of the examined jurisdictions has left the matter unregulated at the legislative level – a gap that, as the following section demonstrates, remains Ukraine's defining characteristic.

Legal regulation in Ukraine: A systemic analysis. Ukrainian legislation does not provide for fingerprinting as a condition of entry into public service for any category of servant. The Law of Ukraine "On Civil Service"[1], in determining the conditions of entry into civilian civil service, contains no provision for the collection of biometric data. The Law of Ukraine "On the National Police"[2], in establishing the requirements for candidates for service (Art. 49) and the procedure for verifying a candidate (Art. 50), similarly does not provide for fingerprinting upon entry. For military personnel, the corresponding statutory norm is also absent.

The existing subordinate regulatory acts in the sphere of dactyloscopy regulate exclusively the fingerprinting of detained, suspected, and convicted persons within the framework of criminal registers, but not of servants upon entry. As Knyzhenko and Sharaban (2023) note, the rules governing the collection, storage, use, and destruction of biometric data are elaborated only in subordinate normative acts, between which there are significant contradictions, and many questions remain unresolved at the legislative level. The entire normative basis in the sphere of fingerprinting in Ukraine relates exclusively to persons in conflict with the law, not to persons entering the ranks of the public service.

The nearest functional analogue of a fingerprint check in the national system is the institution of special verification conducted by the National Agency on Corruption Prevention (NACP). However, it differs fundamentally from biometric identification verification: it is conducted primarily on the basis of documents provided by the person concerned; it relies on a name-based check, not on biometric identification; and it does not cover verification of the identity of the person from the perspective of the correspondence of the documents presented. The absence of a biometric element leaves a systemic risk – the use of forged documents or multiple identities upon entry to public service – that is particularly significant given the established practice of the penetration of foreign intelligence agents into organs of state authority.

Russia's full-scale armed aggression made especially acute the problem of identification of the fallen. Resolution No. 1214 of the Cabinet of Ministers of Ukraine[3] approved the Procedure for Implementing the Experimental Project on Identification of the Remains of Those Killed by Biometric Data, providing for the voluntary fingerprinting of living military personnel for the purposes of post-mortem identification. On 4 December 2025, the Verkhovna Rada approved in the first reading Draft Law No. 14095[4], providing for the use of digitised fingerprints for the identification of the remains of the fallen (ZMINA, 2025). Forensic experts note a fundamental inconsistency: dactyloscopy has not yet been recognised in Ukraine as an independent method of identification, and the identification of the fallen is conducted primarily through DNA analysis, which may take up to fourteen months (MIHR, 2024). As of early 2026, more than 90,000 persons were considered missing in connection with the war.

The question of introducing mandatory fingerprinting of civil servants had already been considered in Ukraine in 2012, when a corresponding draft law[5] was submitted to the Verkhovna Rada. The draft law did not receive legislative realisation, inter alia owing to the absence of an informed-consent mechanism and a clear legal distinction between criminal and administrative registration. This experience underscores the need for the correct positioning of biometric registration as an administrative, not a criminal, instrument. The comparative characteristics of legal regulation across the examined jurisdictions are summarised in Table 1. The comparative data presented in Table 1 permit the following interim conclusions regarding the international regulatory landscape. First, the existence of a comprehensive statutory framework for the biometric registration of public servants is the norm, not the exception, in the jurisdictions examined: the

[1] Law of Ukraine No. 889-VIII "On Civil Service". (2015, December). Retrieved from https://zakon.rada.gov.ua/laws/show/889-19.
[2] Law of Ukraine No. 580-VIII "On the National Police". (2015, July). Retrieved from https://zakon.rada.gov.ua/laws/show/580-19.
[3] Resolution of the Cabinet of Ministers of Ukraine No. 1214 "On the Approval of the Procedure for Implementing the Experimental Project on Identification of the Remains of Those Killed as a Result of the Armed Aggression of the Russian Federation Against Ukraine by Means of Biometric Data". (2025, September). Retrieved from https://legal100.org.ua/yak-teper-budut-identyfikovuvaty-zagyblyh-vijskovyh-postanova-km-ukrayiny-%E2%84%96-1214/.
[4] Draft Law of Ukraine No. 14095 "On Amendments to Certain Legislative Acts of Ukraine Regarding the Identification of Persons Missing under Special Circumstances". (2025, December). Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/45478.
[5] Draft Law of Ukraine "On the Identification of a Person by Means of Fingerprinting". (2012, December). Retrieved from https://ips.ligazakon.net/document/GF7IC00A.

USA, EU member states, Moldova, and Kazakhstan have all enacted primary legislation governing the conditions, scope, and oversight of fingerprint data collection in the public administration context. Second, the differentiated approach – calibrating the intensity of biometric registration requirements to the sensitivity of the position – has emerged as the dominant regulatory model across EU member states, balancing legitimate public-interest objectives against the enhanced protection that Article 9 GDPR requires for biometric data. Third, the continuous monitoring mechanism (Rap Back) implemented in the United States demonstrates that biometric registration is not a one-time event at the point of entry to service, but may extend to the duration of the employment relationship where national security considerations so require. Fourth, the stark contrast between the regulatory completeness of all examined foreign jurisdictions and the complete absence of any statutory framework in Ukraine confirms the characterisation advanced in the preceding analysis: the Ukrainian legal vacuum is not a matter of degree but of kind. Fifth, the table also reveals that the protective guarantees accompanying registration – data retention limits, independent oversight, rights of access and erasure – are constitutive elements of lawful registration regimes, not optional additions; their absence in any future Ukrainian framework would render it incompatible with ECtHR and CJEU standards from the outset.

Table 1. Comparative characteristics of the legal regulation of fingerprinting of public servants

Criterion	USA	EU member states (majority)	Ukraine
Legislative basis	Privacy Act 1974[1]; OPM regulations; 8 U.S.C. § 1440f[2]	GDPR[3] Art. 9(2)(g) + special laws of member states	Absent for public servants
Fingerprinting of civil servants upon entry	Mandatory for all federal servants	Differentiated by security clearance level	Not provided for by any act
Fingerprinting of police and security personnel upon entry	Mandatory	Mandatory in the majority of member states	Not provided for by any act
Fingerprinting of military personnel upon entry	Mandatory (since 1905; hiatus 1974-1990s)	Regulated by national legislation	Voluntary, exclusively for identification purposes (from Sept. 2025)
Continuous monitoring (Rap Back)	Yes (FBI NGI Rap Back)	Limited; varies by member state	Absent
Data retention period	Extended, pursuant to Privacy Act	Limited; right to erasure (GDPR)	Not regulated for servants
Protective guarantees	Privacy Act, CJIS Security Policy	GDPR, independent data protection authorities, ECtHR	Fragmentary; primarily subordinate MIA acts

Source: compiled by the authors on the basis of the sources cited

Discussion

The established legal vacuum in the sphere of fingerprint registration of public servants in Ukraine is not merely a technical shortcoming – it is a structural vulnerability of the public administration integrity system. Verification of a person's identity upon entry to service through a name-based check is a fundamentally less reliable mechanism in comparison with biometric identification, since it does not exclude the possibility of the use of forged documents, substitution of identity, or concealment of a criminal past through a change of identifying data. In this context, the conclusion of S. Knyzhenko & O. Sharaban (2023) that the legal norms in the sphere of the collection of biometric data "contain many contradictions" and "many questions remain unresolved at the legislative level" acquires a qualitatively broader significance – as a characterisation not only of the criminalistic systems of the MIA, but of the public servant verification system as a whole.

The approach to the problem through the prism of an apparent incompatibility of security needs and GDPR requirements is doctrinally erroneous. The construction of Art. 9(2)(g) GDPR directly provides for the processing of biometric data in cases where it is necessary for reasons of substantial public interest on the basis of the legislation of a member state. Thus, the GDPR does not prohibit mandatory fingerprinting of public servants – it establishes quality standards for such regulation. These standards require: a clear legislative basis; a defined and proportionate aim; individual justification in each specific case; a limited retention period; and an effective review mechanism. Under these conditions,

[1] Privacy Act of 1974, 5 U.S.C. § 552a. (1974, December). Retrieved from https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf.
[2] 8 U.S. Code § 1440f "Fingerprints and Other Biometric Information for Members of the United States Armed Forces. Legal Information Institute". (2008, June). Retrieved from https://www.law.cornell.edu/uscode/text/8/1440f.
[3] General Data Protection Regulation. (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

mandatory fingerprinting of public servants, properly enshrined in statute, meets the proportionality principle, provided that a differentiated approach is applied correlating requirements with the level of official powers, access to confidential information, and the potential risk of abuse.

The general GDPR-compatible framework for biometric data processing, yet their analyses predate the CJEU ruling in Comdribus[1], which materially tightens the individual-justification requirement for each data-collection decision. S. Knyzhenko & O. Sharaban (2023) identified internal contradictions within Ukraine's MIA dactyloscopic registers but confined their analysis to the criminal context; the present Article demonstrates that the same structural deficiency extends to the entire public administration verification system. B. Loomis & K. Bowerman (2025) documented NATO's operational biometric capabilities without addressing the national legislative vacuum that makes Ukraine's military identification crisis particularly acute. The MIHR (2024) and ZMINA (2025) reports provide empirical grounding for the legislative urgency established here. Unlike prior scholarship, the present study synthesises the administrative-law, human rights, and wartime-identification dimensions into a unified conceptual framework oriented toward a concrete legislative proposal.

The practice of applying fingerprinting in Ukraine exclusively in the criminal context forms a stable association of this procedure with suspicion of the commission of a crime. The failure of the 2012 draft law[2] demonstrates that the absence of a conceptual distinction between criminal and administrative dactyloscopy is a real factor of social resistance. Overcoming this barrier requires: a clear normative distinction between the two forms of registration; transparent legislative entrenchment of the aims and guarantees; and active public legal awareness work. It is noteworthy that a change in social perception is already occurring in the context of the identification of the fallen: Resolution No. 1214[3] and Draft Law No. 14095[4] were met with public support – because their aim is clearly formulated and understandable (ZMINA, 2025).

The introduction of a system of fingerprinting of public servants requires technical readiness that is as of 2026 insufficient. The existing system of automated fingerprint records of the MIA requires technical improvement and legal regulation, and the MIA databases contain cases of improper deletion of information (Knyzhenko & Sharaban, 2023). The introduction of a new system will require the modernisation of fingerprint collection equipment, improvement in the cyber-protection of databases, establishment of inter-agency information exchange, and personnel training. An existing potential is available: the State Migration Service of Ukraine retains the digitised fingerprints of the thumbs of approximately 35 million citizens, collected during the processing of foreign travel passports – this infrastructure is already being used for the identification of the fallen and may form the basis for a broader system.

The foregoing discussion warrants the following interim conclusions regarding the practical and normative challenges of introducing biometric registration in Ukraine. First, the perception of fingerprinting as exclusively a criminal-law instrument constitutes the principal socio-legal barrier to reform and must be overcome through explicit statutory differentiation between criminal and administrative registration regimes. Second, the failure of the 2012 draft law demonstrates that legislative proposals in this sphere require not only technical legal drafting but also a clearly articulated public justification grounded in identified administrative objectives rather than security rhetoric. Third, the existing biometric infrastructure of the State Migration Service – retaining the digitised fingerprints of approximately 35 million Ukrainian citizens – represents a ready-made technical foundation that significantly reduces the resource cost of implementing a broader registration regime. Fourth, the technical shortcomings of the current MIA dactyloscopic records system (internal contradictions, improper deletions, absence of inter-agency data exchange protocols) must be addressed as a prerequisite condition, rather than a concurrent undertaking, of any legislative expansion. Fifth, the wartime identification dimension – already partially addressed by Resolution No. 1214[5] and Draft Law No. 14095[6] – provides both a normative precedent and a compelling public justification for the adoption

[1] Judgment of the Court of Justice of the European Union in Case No. C-371/24 "Comdribus". (2026, March). Retrieved from https://curia.europa.eu/site/upload/docs/application/pdf/2026-03/cp260039en.pdf.
[2] Draft Law of Ukraine "On the Identification of a Person by Means of Fingerprinting". (2012, December). Retrieved from https://ips.ligazakon.net/document/GF7IC00A.
[3] Resolution of the Cabinet of Ministers of Ukraine No. 1214 "On the Approval of the Procedure for Implementing the Experimental Project on Identification of the Remains of Those Killed as a Result of the Armed Aggression of the Russian Federation Against Ukraine by Means of Biometric Data". (2025, September). Retrieved from https://surl.li/jggfhi.
[4] Draft Law of Ukraine No. 14095 "On Amendments to Certain Legislative Acts of Ukraine Regarding the Identification of Persons Missing under Special Circumstances". (2025, December). Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/45478.
[5] Resolution of the Cabinet of Ministers of Ukraine No. 1214 "On the Approval of the Procedure for Implementing the Experimental Project on Identification of the Remains of Those Killed as a Result of the Armed Aggression of the Russian Federation Against Ukraine by Means of Biometric Data". (2025, September). Retrieved from https://surl.li/jmwxin.
[6] Draft Law of Ukraine No. 14095 "On Amendments to Certain Legislative Acts of Ukraine Regarding the Identification of Persons Missing under Special Circumstances". (2025, December). Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/45478.

of a comprehensive statutory framework, demonstrating that the social perception of biometric registration is already evolving in Ukraine in the direction required for broader reform.

Conclusions

The comparative legal analysis conducted in this Article warrants the following conclusions. In leading democracies – the USA and EU member states – mandatory fingerprinting of public servants upon entry to service is an established instrument implemented on a statutory basis, in compliance with proportionality and personal data protection standards. The American model combines mandatory entry-level biometric registration with continuous Rap Back monitoring; the EU model applies a differentiated approach calibrated to the sensitivity of the position.

Ukraine has no statutory provision for fingerprinting of civil servants, police officers, or military personnel upon entry to service. The entire national dactyloscopic normative framework is confined to the criminal context. This gap constitutes a structural vulnerability of the public administration integrity system, with practical consequences including the risk of identity fraud, concealment of disqualifying backgrounds, and – in the wartime context – the inability to rapidly identify fallen military personnel by biometric means.

The ECtHR standards (S. and Marper, Gaughran) and the CJEU standard (Case C-371/24) do not prohibit mandatory fingerprinting of public servants. They impose four quality requirements: a statutory basis, a specific and proportionate aim, a limited data retention period, and an effective review mechanism. A properly designed Ukrainian law can satisfy all four requirements simultaneously. Russia's full-scale armed aggression has given the fingerprinting question a critical wartime dimension. Resolution No. 1214 of the Cabinet of Ministers and Draft Law No. 14095 represent first normative steps, but the voluntary character of registration and the non-recognition of dactyloscopy as an independent identification method remain systemic shortcomings requiring legislative resolution. The primary legislative step is the adoption of a Law of Ukraine "On Biometric Registration" establishing: a closed list of positions subject to mandatory fingerprinting; proportionality-based differentiation of requirements by risk category; clear rules on data retention and access; an independent oversight mechanism; and a phased implementation timeline compatible with the existing State Migration Service biometric infrastructure.

The prospects for further research lie in the development of a draft conceptual model for such a law, drawing on the legislative experience of EU member states that have implemented differentiated biometric registration regimes within the GDPR framework, and in an empirical assessment of the technical readiness of Ukrainian institutions for phased implementation.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Ashbourn, J. (2014). Biometrics in the new world: The cloud, mobile technology and pervasive identity. *Journal of Information Security*, 6(2).
[2] Bennett, C.J. (2010). The privacy advocates: Resisting the spread of surveillance. Cambridge: MIT Press.
[3] Bidniak, H. (2017). Legal regulation of fingerprinting of persons in Ukraine. *Journal of Criminalistics*, 2(28), 446-450. https://nbuv.gov.ua/UJRN/vkk_2017_2_77.
[4] Brownsword, R., & Goodwin, M. (2012). Law and the technologies of the twenty-first century: Text and materials. Cambridge: Cambridge University Press.
[5] datenshutz. (2020). *Dutch DPA imposes fine on company using fingerprint technology for attendance and time registration.* Retrieved from https://www.datenschutz-notizen.de/dutch-dpa-imposes-fine-on-company-using-fingerprint-technology-for-attendance-and-time-registration-4325764/#_ftn1.
[5] De Hert, P., & Sprokkereef, A. (2008). Data protection and the use of biometric data in the EU. In C. Fischer-Hübner, P. Duquenoy, A. Zuccato & L. Martucci (Eds.), *The future of identity in the information society* (*IFIP Advances in Information and Communication Technology, Vol. 262)* (pp. 213-228). Karlstad: Springer. doi: 10.1007/978-0-387-79026-8_19.
[6] Federal Bureau of Investigation. (2023). *National fingerprint-based background checks: Steps for success*. Retrieved from https://www.fbi.gov/file-repository/cjis/steps-for-success.pdf.
[7] Haggerty, K.D., & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622. doi: 10.1080/00071310020015280.
[8] Jain, A.K., Ross, A.A., & Nandakumar, K. (2011). *Introduction to biometrics*. New York: Springer. doi: 10.1007/978-0-387-77326-1.

[9] Kindt, E.J. (2013). *Privacy and data protection issues of biometric applications: A comparative legal analysis*. New York: Springer. doi: 10.1007/978-94-007-7522-0.
[10] Knyzhenko, S., & Sharaban, O. (2023). Fingerprint registration in Ukraine: Legal regulation and development trends. *Scientific Bulletin of Uzhhorod National University: Law Series*, 2(79), 237-244. doi: 10.24144/2307-3322.2023.79.2.36.
[11] Koops, B.-J., & Leenes, R. (2013). Privacy regulation cannot be hardcoded: A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, 27(1-2), 159-171. doi: 10.1080/13600869.2013.764010.
[12] Loomis, B., & Bowerman, K. (2025). Anonymous no more: Countering the gray zone threat through biometrics-enabled intelligence. *Military Intelligence Professional Bulletin*. Retrieved from https://www.lineofdeparture.army.mil/Journals/Military-Intelligence/Military-Intelligence-Archive/Continuous-Transformation-Special-Edition/Anonymous-No-More/.
[13] Lyon, D. (2009). Identifying citizens: ID cards as surveillance. Ontario: Polity.
[14] Media Initiative for Human Rights. (2024). *How to accelerate the identification of those killed or missing in the war*. Retrieved from https://mipl.org.ua/en/how-to-accelerate-the-identification-of-those-killed-or-missing-in-the-war/.
[15] Mordini, E., & Tzovaras, D. (Eds.). (2012). *Second generation biometrics: The ethical, legal and social context*. New York: Springer. doi: 10.1007/978-94-007-3892-8.
[16] National Research Council. (2010). *Biometric recognition: Challenges and opportunities*. Washington: The National Academies Press. doi: 10.17226/12720.
[17] Orlov, Y. & Pribytkova, N.O. (2022). War and criminal law policy of Ukraine: Challenges and responses. *Law and Safety*, 85(2), 40-49. doi: 10.32631/pb.2022.2.04.
[18] Solove, D.J., & Schwartz, P.M. (2019). *Privacy law fundamentals*. Portsmouth: International Association of Privacy Professionals.
[19] U.S. Army. (2022). *Army unveils new Army Biometric Program Directive*. Retrieved from https://www.army.mil/article/262016/army_unveils_new_army_biometric_program_directive.
[20] U.S. Department of Defense. (2023). *DoD biometrics enterprise strategy 2025-2030*. Retrieved from https://www.defense.gov/Portals/1/Documents/pubs/DoD-Biometrics-Enterprise-Strategy.pdf.
[21] U.S. Department of the Interior. (2023). *Personnel security and credentialing services*. Retrieved from https://www.doi.gov/ibc/personnel-security-and-credentialing-services.
[22] U.S. Office of Justice Programs. (1982). *Abandonment of fingerprint identification by United States Department of Defense* (NCJ 77543). Retrieved from https://www.ojp.gov/ncjrs/virtual-library/abstracts/abandonment-fingerprint-identification-united-states-department.
[23] Westin, A.F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453. doi: 10.1111/1540-4560.00072.
[24] Zakharov, V., & Rudeshko, V. (2015). Biometric technologies in the 21st century and their use by law enforcement (2nd ed.). Lviv: LvDUVS.
[25] ZMINA – Media Initiative for Human Rights. (2025). *How Ukraine searches for and identifies the missing during the war*. https://zmina.info/instructions/yak-v-ukrayini-shukayut-ta-identyfikuyut-znyklyh-bezvisti-pid-chas-vijny-vidpovidi-na-poshyreni-pytannya/.
[26] Zouhar, L., & Bartoszewicz, M.G. (2022). The smoking gun: How gun policies influence types of firearms involved in violent crimes in the Czech Republic and the United Kingdom. *International Journal of Offender Therapy and Comparative Criminology*, 67(10-11), 1180-1199. doi: 10.1177/17488958221134059.
[27] Zwanenburg, M. (2012). International humanitarian law and the use of biometric data. In E. Mordini & D. Tzovaras (Eds.), *Second generation biometrics: The ethical, legal and social context* (pp. 275-294). New York: Springer. doi: 10.1007/978-94-007-3892-8_13.

Біометрична реєстрація державних службовців: між державною безпекою та правом на приватність

Микола Комiссаров
Кандидат юридичних наук, доцент
Центр внутрішньої безпеки спеціального призначення «Гард»
Національної гвардії України
03151, вул. Святослава Хороброго, 9А, м. Київ, Україна
https://orcid.org/0000-0001-6828-7974
Наталя Комiссарова
Кандидат юридичних наук, доцент
Київський інститут Національної гвардії України
03180, вул. Оборони Києва, 7, м. Київ, Україна
https://orcid.org/0000-0001-6895-6891

■ **Анотація.** Статтю присвячено правовому регулюванню обов'язкового дактилоскопіювання державних службовців як механізму верифікації особи, забезпечення доброчесності та безпеки публічного управління. На основі порівняльно-правового та формально-юридичного методів проаналізовано законодавство України, держав-членів Європейського Союзу та Сполучених Штатів Америки щодо збирання й оброблення дактилоскопічних даних осіб, які обіймають або претендують на посади публічної служби. Систематизовано практику Європейського суду з прав людини у справах S. and Marper v. United Kingdom, Gaughran v. United Kingdom та рішення Суду справедливості Європейського Союзу у справі C-371/24 Comdribus. За результатами встановлено, що в Україні дактилоскопіювання під час вступу на публічну службу не передбачене жодним нормативно-правовим актом – ні для цивільних службовців, ні для поліцейських, ні для військовослужбовців, – що становить структурну вразливість системи доброчесності публічного управління. Підхід, відповідно до якого GDPR забороняє таку реєстрацію, визнано доктринально хибним: ст. 9(2)(g) GDPR прямо допускає обробку біометричних даних з мотивів суттєвого суспільного інтересу за наявності належної законодавчої основи. Обґрунтовано диференційовану модель запровадження дактилоскопіювання відповідно до стандартів Європейського суду з прав людини, Суду справедливості Європейського Союзу та GDPR. Виявлено специфічний вимір проблеми – ідентифікацію загиблих військовослужбовців – та запропоновано його нормативне вирішення. Сформульовано висновок, що ухвалення Закону України «Про біометричну реєстрацію» з диференційованим підходом до категорій посад, чіткими гарантіями захисту персональних даних і поетапним запровадженням є першочерговим законодавчим кроком

■ **Ключові слова:** біометрична реєстрація; захист персональних даних; доброчесність державної служби; право на приватність; ідентифікація загиблих