8.

Vojkan Nikolić[1]
Nikola Petrović[2]

INFORMATION SYSTEMS FOR MONITORING MIGRATION FLOWS AND SECURITY IMPLICATIONS

DOI:10.5937/BINS26082N

Abstract

This paper examines the use of information systems in monitoring migration flows, with particular attention to the link between operational efficiency, cybersecurity and the protection of people involved in migration procedures. The subject is not treated as a simple matter of border surveillance. It is approached as a problem of data management across several actors, including border authorities, asylum bodies, reception centres, health services and humanitarian organisations. The paper uses publicly available data from UNHCR, IOM, Frontex and Eurostat to show why timely and verifiable data processing has become relevant for decision-making. It proposes a modest operational matrix that connects data categories, possible security value and mandatory safeguards. The contribution is not presented as a new software solution, but as a practical way of assessing whether existing or future systems balance institutional needs with the protection of sensitive personal data.

Keywords*: migration flows, information systems, cybersecurity, interoperability, data protection*

Introduction

Migration flows are often described through numbers: how many people crossed a border, how many applied for asylum, how many were accommodated in reception centres. These numbers are necessary, but they do not say enough on their own. Behind them are different situations: people escaping war, families seeking protection, persons in transit, and networks that exploit insecurity for profit. For that reason, information systems in this field cannot be treated as ordinary administrative registers. In contemporary states, migration data are produced in several places. A border authority records a crossing or an attempted crossing. An asylum authority manages a procedure. A reception centre keeps information on accommodation and immediate needs. A health service may hold urgent information that matters for the protection of life but should not be widely shared. If these data remain isolated, institutions react late or on the basis

[1] University of criminal investigation and police studies, Belgrade, Serbia, vojkan.nikolic@kpu.edu.rs
[2] Ministry of the Internal Affairs, Belgrade, Serbia, nikola.spetrovic@mup.gov.rs

of a partial picture. If they are connected without rules, the risk shifts toward excessive surveillance and misuse. This is also a legal, not only technical, question. The GDPR requires personal data to be collected for specified and legitimate purposes and to be limited to what is necessary for those purposes, while Regulation (EU) 2024/1351 places migration management within a wider framework of responsibility, coordination and solidarity between competent authorities (Regulation (EU) 2016/679, 2016; Regulation (EU) 2024/1351, 2024). The question addressed in this paper is therefore practical: how can a system for monitoring migration flows help institutions work faster and more accurately without turning sensitive data into an instrument of uncontrolled control? The answer is not only a matter of technology. The same database, GIS layer or analytical module may be useful or harmful depending on who has access, what is stored, for how long, on what basis decisions are made and whether later review is possible.

The paper is written as an analytical review with a conceptual contribution. It first explains why migration is demanding from the standpoint of data management. It then discusses core technological components, security risks and interoperability. The final part proposes an operational matrix that can be used to check whether a system gives equal attention to security, individual protection and institutional accountability.

Migration as a Data Issue, Not Only Movement of People

The visible part of migration takes place on the ground: border crossing, registration, transport, accommodation and interviews with officials. Less visible is the flow of data that follows every one of these actions. That flow often determines whether a decision will be made in time, whether a person will receive appropriate protection and whether services will notice a security risk before it becomes more serious. The typical problem is not a complete lack of information, but fragmentation. One part of the data may be in a police record, another in an asylum case file, a third in a reception register, and a fourth in reports prepared by international organisations. When data are entered manually or exchanged through informal channels, every next institution receives the picture with a delay. In ordinary conditions this causes administrative difficulties. During pressure periods it may have more serious effects: poor capacity planning, missed protection of minors, or late detection of organised groups using the same routes. The opposite risk should not be ignored. Migration data are not ordinary statistical entries. They often include identity, biometrics, family relations, location, legal status and indicators of vulnerability. For people who have fled persecution, such a set of data may be dangerous if it reaches the wrong actors. A migration information system therefore needs a double logic: it must be connected enough to prevent institutions from working blindly, but restricted enough so that each actor sees only what is necessary for its task. It is useful to distinguish three levels of data. The first is the operational level, where officials

work with specific cases and identities. The second is the analytical level, where patterns are observed by time, route and type of event. The third is the strategic level, where capacity and policy responses are planned. Mistakes occur when these levels are mixed, for example when individual data are used for broad analysis without protection, or when aggregated data are treated as proof of risk in an individual case.

Data and Methodological Approach

The paper relies on publicly available sources because they provide a verifiable basis for discussing system requirements. It uses global data from IOM and UNHCR, Frontex data on detections of irregular crossings at the external borders of the European Union, and Eurostat data on first-time asylum applicants (IOM, 2024; UNHCR, 2025; Frontex, 2025; Eurostat, 2025). These sources do not provide a complete field picture, but they are sufficient for testing the main assumption of the paper: a migration information system has to process statistical volume, individual casework and data-security risk at the same time.

Table 1. *Indicative public data relevant to migration flow monitoring*

Source	Data point	Relevance for an information system
IOM, World Migration Report 2024	About 281 million international migrants worldwide in 2020.	Shows the scale of the phenomenon and the need for stable records rather than ad hoc reporting.
UNHCR, Global Trends 2024	123.2 million forcibly displaced people at the end of 2024.	Shows that migration data often involve humanitarian and legal protection, not only administration.
Frontex, 2024	239,159 detections of irregular border crossings at EU external borders; 38% decrease from 2023.	The system has to distinguish an overall decrease from shifts in routes and methods.
Frontex, Western Balkan route 2024	21,520 detections; 78% decrease.	For countries on the route, local patterns matter more than a general European average.
Eurostat, 2024	912,000 first-time asylum applicants in the EU, 13% fewer than in 2023.	Connects border data with later administrative procedures and asylum capacity.

Source: *Author's presentation based on IOM (2024), UNHCR (2025), Frontex (2025) and Eurostat (2025).*

The figures in the table should be read carefully. A decrease in detections on one route does not mean that risk has disappeared. Movement may have shifted, smuggling

methods may have changed, or controls may have had different effects than before. Similarly, asylum applications do not describe all migration. Some people never apply, some remain in transit, and some enter through regular channels. A system should not treat a single indicator as final evidence. Methodologically, the paper combines a functional analysis of information systems with risk analysis. It first asks what the system should enable: recording, verification, spatial display, exchange and analytical processing. It then asks what may go wrong with each function. This is more practical than a general list of technologies, because the same technical component can have very different value depending on how it is introduced and used.

Technological Components of the System

In an operational environment, a system for monitoring migration flows is rarely a single application. It is more often a set of services: a case register, an identification module, a GIS layer, a data-exchange service, a user portal and an analytical dashboard. The need to process heterogeneous and fast-moving data is also visible in smart-city security contexts, where OSINT sources and Hadoop-based analytics have been used to support rapid person identification and scalable data processing (Petrović & Nikolić, 2025). These components exchange events, case statuses and spatial records, usually through an API layer or scheduled synchronisation. If that layer is not documented clearly, errors do not appear immediately in the interface; they appear later, when two authorities work with different statuses for the same person.

Table 2. *Typical system components and points of risk*

Component	Operational function	Risk if the control is poorly configured
Case register	Records status, accommodation, procedure stage and basic identifiers.	Overly broad case access or incorrect identity merging.
GIS layer	Displays routes, pressure points and event clusters over time.	Tracking an individual instead of an aggregated spatial trend.
Biometric check	Deduplicates records and verifies identity through a controlled query.	Exposure of non-changeable data or unauthorised reuse.
Analytical dashboard	Signals deviations, route shifts and repeated patterns.	Automatic judgement without human review or explanation of the signal.
API/data exchange	Exchanges status and minimum attributes between competent authorities.	Uncontrolled data sharing and inconsistent access rules.

Source: *Author's presentation*

The case database remains the most sensitive point of the system. It combines identifiers, procedure status, accommodation history, field notes and, in some cases, biometric or health-related attributes. The technical issue is not only data storage, but also data linkage. A poorly configured deduplication mechanism may merge two different identities, while an overly broad query may display more information than the user needs for the task at hand. The analytical module often receives the most attention, especially when it is used to detect route shifts, unusual crossing frequencies or repeated use of the same logistical points. Its output should not be treated as a decision, but as a signal for review. A useful dashboard therefore does not display only a risk label; it also provides a basic trace: time period, geolocation cluster, event type and confidence level. Without that trace, analytics becomes a black box and the official receives a feeling of precision that cannot be checked. For end users, the GUI is decisive because it shapes the quality of data entry. If a form contains too many mandatory fields, the official will often choose the fastest option rather than the most accurate one. If the system does not separate operational entry from analytical review, the same user may easily gain access to data that are not necessary for the task. For that reason, work screens, the administration panel, audit view and analytical dashboard should be separated from the start.

What the System Can Detect, and What It Must Not Assume

Information systems can be useful in the early detection of patterns. A sudden route change, repeated use of the same contact points, an unusual number of unaccompanied minors or unexpected pressure on a reception centre may require a response. These signals are not evidence by themselves, but they help direct attention and resources to places where review or assistance is more urgently needed. In relation to human trafficking and migrant smuggling, analytics must not become rough profiling. A person coming from a particular country or moving along a particular route should not be treated as a risk for that reason alone. More useful are behavioural and situational indicators: dependence on the same intermediaries, inability to explain the journey, signs of coercion, family separation, or frequent changes in the account of events. Even these indicators have to be interpreted carefully, because fear and trauma can also affect a person's statements. The system can also support humanitarian response. If the number of families with children increases over a short period, the total number of people is not enough. Information is needed on structure, duration of stay, available accommodation and services. This shows the difference between control and management. Control records that an event has taken place. Management tries to anticipate the next practical problem: food, transport, medical support, interpretation, legal counselling or safe accommodation. The limits of the system should be stated clearly. It cannot assess the truth of a life story by itself, replace an interview with an official, or solve the political causes of migration. Its

realistic value is more modest, but still important: it reduces information delays, connects services that otherwise work separately and leaves a trace of how a decision was made.

Cybersecurity and Protection of Sensitive Data

Cybersecurity in migration systems is not an additional technical issue to be solved at the end of a project. It determines whether the system can be legitimate at all. If one database contains identity, location, biometrics, family links and procedure status, a data breach may have consequences more serious than in many other public registers. The damage would not be only administrative. A person could be exposed to retaliation, blackmail, discrimination or information being returned to actors from whom they fled.

Alignment with the RBAC (Role-Based Access Control) model means that a reception-centre operator sees, through the graphical user interface (GUI), only accommodation status, interview schedule and basic contact information, while asylum case-file elements, medical history or biometric templates are masked by the system. An analyst may see aggregated spatial and temporal patterns without seeing a person's full name. A system administrator maintains accounts and permissions, but should not have unrestricted access to case content. This separation is not a formality. Similar role-limited access is important in mobile intranet environments, where a WireGuard-based model can connect field users through a controlled gateway while peer-specific addresses, AllowedIPs and firewall rules restrict access according to operational roles (Petrović et al., in press). It is the practical translation of GDPR principles such as purpose limitation, data minimisation, accuracy, integrity, confidentiality and accountability into daily system use (Regulation (EU) 2016/679, 2016). Biometrics require a stricter regime than ordinary identity data. In a practical configuration, the biometric template is separated from the basic case file, encrypted both at rest and in transit, and never displayed as raw biometric data to the application user. The user should see the verification result, such as a confirmed match or a warning about a possible duplicate entry, not a data element that cannot be changed if it is exposed. Insider misuse is a real risk, especially when several services use the same system. The audit log should therefore record not only failed login attempts, but also case views, data exports, status changes, permission changes and manual identity merges. Simple anomaly rules may also be useful, for example an alert when a user opens a large number of cases in a short period without a link to that user's organisational unit. This is not a substitute for an investigation, but it is an early signal that access should be reviewed. Reliability concerns are also present in intrusion-detection systems, where threshold determination and redundancy mechanisms can reduce false signals and improve the stability of security decisions (Maksimović et al., 2024).

Interoperability and Exchange Between Institutions

Interoperability is often presented as a technical requirement, but in this field it has security, legal and humanitarian value as well. If systems do not exchange data, a person may go through the same procedure several times, while services may make decisions without knowing relevant earlier events. If exchange exists but is not regulated, the risk only moves elsewhere: data travel faster, but no one knows who saw them and why. A good exchange model does not have to mean one large central database for everyone. In many cases, it is better for institutions to keep their own records while exchanging limited and standardised data sets through controlled services. This reduces the need to copy entire case files. Earlier work on e-government services in the crime domain also shows that timely institutional responses depend on structured information exchange and clearly modelled service workflows (Nikolić et al., 2017). For example, one institution can confirm that a case exists and indicate its status without disclosing all details to every user who sends a query. This approach is consistent with Regulation (EU) 2024/1351, which treats asylum and migration management as a coordinated system of responsibility and solidarity rather than a set of isolated national procedures (Regulation (EU) 2024/1351, 2024). Standardisation of terms is less attractive than artificial intelligence, but often more important. If one service uses 'registration' to mean first contact, another uses it for biometric verification and a third for opening an official procedure, aggregate reports will not be reliable. The same applies to statuses such as 'in transit', 'accommodated', 'referred', 'left the centre' or 'vulnerable category'. A system needs a common vocabulary used by all participants. Secure data exchange also requires institutional discipline. In crisis situations there is often pressure to share everything with everyone. This may look efficient, but in the long run it undermines trust and increases the risk of error. A better approach is to define in advance which data are shared, with whom, in which situation, under which legal basis and for how long they are retained.

Operational matrix as the contribution of the paper

The contribution of this paper is not a new algorithm or a finished system architecture. That would be too ambitious for a paper of this scope. The proposal is simpler: an operational matrix through which each system function is checked by three questions. What is the smallest amount of data needed? What is the concrete security or humanitarian value? What control prevents the data from being used more broadly than justified?

Table 3. *Operational matrix for balancing security and rights protection*

System question	Minimum data needed	Required control
Has the person already been recorded?	Case identifier and limited identity markers.	Duplicate check without broad disclosure of personal data.
Is the route changing quickly?	Aggregated spatial data by point and period.	Anonymisation or aggregation where individual identity is not needed.
Is there a smuggling risk?	Movement pattern, frequency and linked events.	Human review before any operational decision.
Is the person particularly vulnerable?	Age, family status, health or protection note.	Strictly limited access and a log of every consultation.
Does the system produce errors?	Records of corrections, appeals and later changes.	Audit log, periodic review and a right to correction.

Source: *Author's presentation*

The matrix is intended as a working tool for system design or review. Its value lies in forcing system designers to explain the purpose of processing before adding a new function. If a function cannot be connected with a minimum data set and a safeguard, it is probably not sufficiently justified. This matters especially in risk analytics, where there is a temptation to collect more data on the assumption that it might be useful later. For example, when the system signals a route shift, the operational matrix prevents that information from being automatically linked to an individual identity. The first step is aggregation at the level of a geolocation point, or event cluster, while identity is introduced only if additional indicators of a criminal offence, a protection need or a concrete operational procedure exist. In this way, the same information can support situational assessment without unnecessarily widening the circle of personal data. This approach is not spectacular, but it is usable. It can be applied by a small institution introducing a basic register, or by a larger system reviewing existing modules. The matrix does not solve every problem. It does not replace law, data-protection impact assessment or expert security judgement. Its purpose is to organise the most basic question: whether the system uses data for protection and management, or merely accumulates them because technology makes this possible.

Data Quality and the Problem of Incorrect Record Matching

A separate issue in migration records is not only protection, but also data quality. These systems often contain names transliterated from different scripts, uncertain dates of birth, incomplete family links and short notes entered under pressure in the field. If such records are later connected mechanically, the system may produce a neat but inaccurate case file. For the service, this is an operational problem. For the person concerned, it may become a serious legal burden. For that reason, a deduplication module should not rely only on exact matching of first and last names. A more realistic configuration combines a case identifier, a limited set of biometric templates, registration history, first-contact location and controlled manual confirmation by an authorised officer. The system may show that two records are similar, but it should not merge them automatically without a marked verification step. This reduces the risk that an incorrectly merged record will later influence the asylum procedure, accommodation decisions or a security assessment. Data quality also depends on the design of the interface. If the GUI forces quick entry through drop-down lists without space for a short note, the officer in the field will often choose the closest option, not necessarily the most accurate one. If, on the other hand, the form relies too much on free text, later analysis becomes unreliable. A better solution is a combination of controlled fields and short structured notes, with mandatory logging of who entered the data, when the change was made and what the basis for the change was. In this paper, data quality is treated as part of system security. An inaccurate record is not merely an administrative error. It may lead to a wrong allocation of resources, unnecessary additional checks, or an unjustified association of a person with a risk pattern. In migration systems this is particularly sensitive because errors can travel between institutions. A wrongly flagged case may continue to appear in data exchange even after the original assumption has been corrected. Practical quality control does not have to be complicated. Mandatory fields should be used only where they are truly needed, the reliability level of individual data elements should be marked, information confirmed by a document should be separated from information obtained through a statement, and high-impact records should be reviewed periodically. Such measures do not slow the system down significantly, but they prevent the digital record from gaining more authority than it deserves.

Operational Flow for Processing a System Signal

The practical value of an information system can be seen more clearly through a typical signal-processing flow. For example, the system may register that, over several days, entries along an alternative route are increasing, while a reception centre reports a larger number of persons mentioning the same gathering point. This is not evidence of smuggling. It is a signal that requires verification, comparison with the previous period

and assessment against other indicators. The first step in such a flow should not be the opening of individual case files, but aggregation. The analytical dashboard should display change by location, time and event type without automatically listing identities. Only if the signal persists and is supported by other sources, such as a field report or accommodation pressure data, should the case move into a more detailed verification mode. In the second step, an officer checks whether the signal is caused by a technical error, a change in recording practice or a real development in the field. This matters because information systems sometimes register changes produced by the system itself: a new input form, delayed synchronisation or a local change in classification may look like a new operational trend. Only the third step may involve broader access to case files, and even then with approval and recorded access. At that point, RBAC rules must distinguish between an operational user, an analyst and a manager. Table 4 presents a simplified signal-processing flow. Its purpose is not to replace an institutional procedure, but to show how technical processing can be linked to data minimisation and verifiable decision-making.

Table 4. *Processing flow of an operational signal in a migration information system*

Phase	What the system does	Control that limits risk
Signal	Displays change by route, time or reception-centre capacity.	Uses aggregated data without automatically opening identities.
Verification	Compares the signal with the previous period and the source of entry.	The audit log shows who entered or changed data and from which module the record came.
Correlation	Connects the signal with other indicators, such as field reports or repeated references to the same contact point.	Correlation does not produce a conclusion of guilt, but only a basis for further checking.
Action	Assigns a task to the competent service or manager.	RBAC determines who may see the case, and each access remains recorded.
Review	Checks afterwards whether the signal was useful or false-positive.	The result of the review is used to adjust rules and reduce future errors.

Source: *Author's presentation*

System Limitations and Conditions for Responsible Implementation

Even a well-designed system cannot remove all limitations. The first limitation is dependence on input data. If data are entered under pressure, without sufficient training or under different local rules, analytics will only display the existing inconsistency in a more organised form. It is therefore misleading to expect that the problem of migration management can be solved by purchasing software. Software helps only when clear procedures already exist. The second limitation concerns the interpretation of risk. Migration flows change because of visa policy, weather conditions, closure of particular routes, the activity of smuggling networks, but also because of rumours that spread quickly among people on the move. The system can register a change, but it does not always know its cause. If every change is immediately treated as a security threat, the result is a large number of false alarms and a loss of trust among system users. The third limitation is institutional unevenness. One service may have a stable network, trained administrators and defined procedures, while another may work with outdated equipment and limited staff. For that reason, the system should be introduced gradually. Modules that are critical for identity and access control should not depend on the most complex analytical functions. Basic recording, access control and audit logging must remain reliable even when an advanced module is unavailable. The fourth limitation concerns the trust of the persons whose data are processed. If a person does not understand why data are collected, to whom they may be forwarded and how long they will be kept, the system may be perceived as a tool of pressure. This does not mean that every technical procedure has to be explained in detail, but the basic purpose of processing must be clear and accessible. Transparency is not only a legal requirement; it is also a practical condition for better cooperation in the field. Responsible implementation therefore rests on several modest but firm rules: collect fewer data when that is sufficient, separate operational work from analytical inference, keep a human in the loop for decisions that may affect an individual, and regularly check who accessed sensitive records. Such rules do not make the system perfect, but they make it more usable and less risky.

Continuity of Operation and Incident-Mode Procedures

A migration information system must be designed for ordinary days, but its real value usually becomes visible during periods of sudden pressure, temporary route closure, field-network outage or cybersecurity incident. If basic recording stops working at that moment, services return to paper lists and later manual re-entry creates duplicate or unreliable records. For that reason, a limited offline or restricted mode can be useful, but only with a minimal data set: time of contact, location, temporary case number and a basic category of need. It should not contain a full asylum file, medical data or broader biometric information. Once the connection is restored, synchronisation should mark

the record as created offline and subject it to later verification. The analytical layer should also display the status of the data source. A sudden drop in registrations may be a real route change, but it may also be the result of a local outage or delayed synchronisation. The recovery plan should therefore distinguish normal mode, restricted mode and recovery mode. Normal mode uses full validation and access controls. Restricted mode narrows the data set and enables basic recording without opening sensitive modules. Recovery mode verifies and marks records created during the interruption. This division improves resilience, but also prevents a crisis from becoming an excuse for unlimited collection and sharing of data.

Discussion

Public data can easily lead to quick conclusions about whether pressure on a route is increasing or decreasing. That is not enough for assessing an information system. A system is not successful simply because it records a lower number of events. It is successful if institutions use its data to recognise change earlier, allocate resources better and reduce harm to people in procedure or in transit. This is particularly relevant for the Western Balkan route. The 78% decrease in detections recorded for 2024 should not be read as proof that regional risk has disappeared; it may also indicate route displacement, changed methods of movement or different control effects. For countries on this route, national and regional systems therefore need controlled interoperability with central European systems, including Eurodac and the Schengen Information System (SIS), while preserving strict data-quality and access-control rules (European Commission, n.d.; eu-LISA, n.d.). The main advantage of digital systems is the speed with which they connect information. Their main weakness is the possibility that speed turns into automatic judgement without context. In migration, context is essential. The same movement pattern may result from organised smuggling, but also from the closure of another route, weather conditions, fear of registration or misinformation circulating among migrants. Analytical output should therefore be treated as a question for review, not as a final answer. Another issue is trust. Migrants often do not know who processes their data, why biometrics are taken and to whom information may be forwarded. If a system cannot explain the purpose of processing in clear terms, it risks losing legitimacy. This does not mean that every operational detail must be public. Basic processing rules, rights of the person and complaint mechanisms must, however, be understandable. A third problem is the uneven capacity of institutions. It is not realistic to expect every service to have the same level of equipment, training and staffing. Systems should therefore be modular. A smaller number of reliable functions that are actually used is better than a large number of modules that exist only on paper.

Conclusion

Information systems for monitoring migration flows can significantly support institutions, but only if they are developed with a clear understanding of the limits of technology. They can speed up data exchange, reduce duplicated records, help detect changes on routes and support capacity planning. They can also help identify vulnerable persons earlier and refer them to appropriate protection. The same systems can cause serious harm if introduced without access control, a clear purpose of processing and review of algorithmic outputs. Biometric data, spatial tracking and analytical risk models are particularly sensitive. Security should therefore not be understood only as border protection or protection of the database against hackers. In this field, security also includes protection of the person whose data are processed. The proposed operational matrix offers a simple way to check each system function before implementation: whether the data are truly needed, whom the function serves and which safeguard follows it. Such an approach may help migration systems become efficient and responsible at the same time. That is probably the central point: an information system in this field should not be only a faster register, but a controlled mechanism for making better, more verifiable and more humane decisions.

Reference List

European Commission. (n.d.). Schengen Information System. Migration and Home Affairs. https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_en

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (n.d.). Eurodac. https://www.eulisa.europa.eu/activities/large-scale-it-systems/eurodac

Eurostat. (2025). First-time asylum applications down 13% in 2024. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250320-1

Frontex. (2025). Annual Brief 2024. European Border and Coast Guard Agency. https://prd.frontex.europa.eu/wp-content/uploads/annual_brief_2024.pdf

Frontex. (2025). Irregular border crossings into EU drop sharply in 2024. European Border and Coast Guard Agency. https://www.frontex.europa.eu/media-centre/news/news-release/irregular-border-crossings-into-eu-drop-sharply-in-2024-oqpweX

International Organization for Migration. (2024). *World Migration Report 2024.* IOM. https://worldmigrationreport.iom.int/

Maksimović, A., Nikolić, V., Vidojević, D., Ranđelović, M., Đukanović, S., & Ranđelović, D. (2024). *Using triple modular redundancy for threshold determination in DDoS intrusion detection systems*. IEEE Access, 12. https://doi.org/10.1109/ACCESS. 2024.3384380

Nikolić, V., Markoski, B., Kuk, K., Ranđelović, D., & Čisar, P. (2017). Modelling the system of receiving quick answers for e-government services: Study for the crime domain in the Republic of Serbia. *Acta Polytechnica Hungarica*, 14(8), 143–163. https://doi.org/10.12700/APH.14.8.2017.8.8

Petrović, N., & Nikolić, V. (2025). Integrating OSINT with Hadoop analytics for rapid person identification in smart-city events. *AlfaTech*, 1(2), 39–43. https://doi.org/10.46793/AlfaTech1.2.39P

Petrović, N., Viduka, D., & Nikolić, V. (in press). Using WireGuard to protect intranet networks on mobile devices. *Sinteza Conference Proceedings*.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, General Data Protection Regulation. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management, amending Regulations (EU) 2021/1147 and (EU) 2021/1060 and repealing Regulation (EU) No 604/2013. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1351/oj

UNHCR. (2025). *Global Trends: Forced Displacement in 2024*. United Nations High Commissioner for Refugees. https://www.unhcr.org/globaltrends