*Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi*
*Sayı 9, S. 109-114, 10, 2025*

***Araştırma Makalesi***

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

*International Journal of Advanced Natural Sciences and Engineering Researches*
*Volume 9, pp. 109-114, 10, 2025*

***Research Article***

# Personal data ethics in forensic informatics: Developing innovative solution methods with TRIZ method

[1]Semih Balcı, [2]Erhan AKBAL

[1]*Department of Digital Forensics Engineering / Graduate School of Natural and Applied Sciences / Fırat University / Turkey*

*(sbalci23@gmail.com)*

[2]*Department of Digital Forensics Engineering / Technology Faculty / Fırat University / Turkey*

*(erhanakbal@firat.edu.tr)*

*(Received: 30 September 2025, Accepted: 01 October 2025)*

(5th International Conference on Frontiers in Academic Research ICFAR 2025, September 25-26, 2025)

**ATIF/REFERENCE:** Balcı, S. & Akbal, E. (2025). Personal data ethics in forensic informatics: Developing innovative solution methods with TRIZ method, *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(10), 109-114.

***Abstract –*** This study addresses the ethical tensions between the protection of personal data and the need for evidence integrity and rapid work in forensics through the TRIZ approach. First, four basic contradictions are defined: confidentiality-access, speed-procedurality, scope-proportionality, and transparency-operational security. Then, feasible solutions are proposed using TRIZ's practical principles. Selective acquisition and automated masking, focusing only on event-relevant data, an ethical compliance matrix based on objective–data mapping. Evidence quarantine and recorded access for sensitive content. Role-based authorizations that are time-bound and can be easily revoked when needed. Records that track all transactions, maintaining integrity. This approach reduces unnecessary personal data exposure, maintains the integrity of evidence, makes decisions visible, and facilitates auditing. Qualitative evaluations show that selective acquisition and masking enable data minimization while accelerating review. It shows that approval and registration flows strengthen defensibility. Proper tool support, team training, and clear corporate policies are important for successful implementation. In the future, it is recommended to develop evaluations with measurable metrics (completion time, mask opening rate, number of access requests), tool integrations, and training programs across different types of cases. This framework offers a streamlined and scalable roadmap that makes it easier to achieve operational goals while adhering to ethical principles.

*Keywords – Forensic Informatics; Personal Data Ethics; TRIZ; Data Minization; Integrity of Evidence; Auditability.*

## I. INTRODUCTION

With the acceleration of digitalization, forensic informatics has turned into a critical area of expertise consisting of incident response, evidence acquisition, analysis and reporting stages. In these processes, personal data is inevitably processed, which brings with it strong ethical responsibilities as well as legal obligations. The main challenge, to reduce the risk of unnecessary personal data processing while ensuring the integrity and accessibility of evidence and to establish a sustainable balance between operational requirements and ethical principles.

In practice, this balance appears in the form of concrete tensions, the need for comprehensive acquisition with the principle of data minimization crime scene pressure and the need for speed, with procedural compliance and recording obligations. Operational secrecy with the expectation of transparency, permanent and broad powers may conflict with flexibility and the risk of abuse of authority. When these contradictions are not clearly structured, decisions are based on personal interpretations and habits this undermines both ethical and technical defensibility. The explainability and auditability of processes are critical, not only because of regulatory requirements, but also for enterprise risk management and quality assurance.

TRIZ is a creative problem-solving approach that aims to solve contradictions systematically. This study proposes a method that makes tensions visible, manageable and controllable by bringing TRIZ's contradiction-centered thinking to the context of personal data ethics in forensic informatics. Our contributions are: (i) structural classification of ethical tensions, (ii) adaptation of TRIZ tools to the judicial workflow, and (iii) design of practical, auditable solution components. Additionally, standardization of processes and alignment of the registry infrastructure with corporate governance supports the sustainability of the proposal.

## II. MATERIALS AND METHOD

### Scope and Assumptions

The scope of this study covers the typical forensic informatics workflow that includes crime scene response, acquisition, preliminary examination, deep analysis, reporting and storage stages. The proposals have been developed at the level of technical principles and process/policy designs, without resorting to the use of figures and tables, and are presented on instrument-independent principles [1]. Among the assumptions, it is accepted that standard toolkits (e.g. disk or mobile imaging, network traffic capture, log analysis) are used, institutions have a minimum level of policies and procedures, and the recording infrastructure can be used for audit purposes.

### Classification of Ethical Tensions

Since personal data processing is inevitable in forensic computing processes, various ethical tensions arise. The tension between privacy and accessibility includes the obligation to protect personal data on the one hand and the need for fast and comprehensive access to evidence on the other [2]. The tension between speed and expediency arises from the time pressure with procedural compliance, registration, and approval imperatives. The tension between scope and proportionality is seen between the need for broad data acquisition and the principle of collecting only necessary and relevant data. The tension between transparency and operational security arises between demands for explainability and accountability and the confidentiality and security requirements of the investigation [3].

### TRIZ Tool Set and Adaptation Principles

The TRIZ approach provides an important framework for resolving these tensions that arise in forensic informatics processes. The Approach to Ideal Outcome (IFR) principle adopts the state of "achieving the goal with no ethical violations, loss of evidence and minimum resources" as the design anchor [4]. Resource analysis ensures that existing technical, processual, and human resources are included in the solution without generating additional risks. The principle of separation and selectivity allows selective acquisition and disclosure with field, time, condition and part-based separations. Dynamic and revocable design creates flexible yet controllable workflows with time-limited and contingent authorizations. Finally, the principle of a self-auditing system makes auditability a core function of process design [5].

### Application Steps

The proposed methodology consists of six steps. In the first step, the workflow is mapped on a stage-by-stage basis; personal data types, purposes, and risks are listed, conflicts are mapped to decision points, and risk levels are labeled [1]. In the second step, the idealized target situation is defined for each contradiction; tools, roles, enrollment infrastructure, policy, and training resources are inventoried. In the third step, the TRIZ principles are mapped to the relevant contradictions. In the fourth step, the solution design is made; In this context, targeted acquisition and masking, ethical compliance matrix, evidence quarantine and auditable access, time-limited authorization and chain control-oriented recording mechanisms are established [2]. In the fifth step, each designed component is evaluated on ethical compliance, evidence integrity, operational efficiency, auditability, training and cost criteria. In the sixth step, processes are improved and metrics are monitored with gradual transition, controlled pilots and feedback loops [3].

### Recommended Solution Components

In this context, five basic solution components are proposed. The first is the targeted acquisition and masking approach data categories associated with the event are predefined, acquisition profiles target these categories, and personal areas are protected by an automatic masking policy during image [4]. Unmasking is only possible with a reasoned request and approval flow. The second component is the ethical compliance matrix and the proportional collection mechanism. This approach adds a systematic proportionality test to collection and storage decisions; In a matrix where intents and data categories intersect, data is labeled as necessary, conditional, or unnecessary. The third component is evidence quarantine and auditable access. Sensitive data is isolated, accesses are linked to a reasoned consent mechanism, and detailed trace records are kept with integrity guarantee [5]. The fourth component is the time-limited and revocable authorization approach. Role-based access is defined as time-limited tokens. Extension requests are limited to evidence-based evaluation and approval processes. The fifth component is the chain control-oriented recording mechanism. The success of the proposed approach is evaluated based on ethical compliance, evidence integrity, operational efficiency, auditability, and applicability.

## III. RESULTS

### Ethical Compliance and Data Minimization

Targeted acquisition and masking practices have significantly reduced the transfer of personal data fields unrelated to the incident to the process. When unmasking is tied to justified request and approval steps, unnecessary access decreases; the threshold of ethical review is rising. The ethical compliance matrix has served as a reference guide in ambiguous situations by making collection and storage decisions visible. This approach supports reproducibility of decisions and institutional standardization.

### Integrity of Evidence and Defensibility

Evidence quarantine has reduced the risk of evidence integrity challenges by isolating sensitive content and recording access. Detailed access logs have made it easier to present the reasons for the decision and the transaction chain clearly during the reporting phase, the plot and decision points were clarified. Chain audit-oriented registration has increased defensibility in internal and external audit processes.

### Operational Efficiency and Agility

Time-limited and revocable authorization has maintained agility without increasing operational delays while tightening access control. Task-based, time-limited powers limit the risks that may arise from permanent broad powers; Selective acquisition profiles have reduced the volume of data processing, focusing analysts attention on event-related datasets. This has improved the balance of review time and workload.

### Transparency of Decision Processes

The ethical compliance matrix and approval flows standardized the writing of justifications at decision points; It has clarified intra-team communication and role boundaries. Standardization of access and transaction records reduced uncertainties in post-verification; It has facilitated the early detection of out-of-process deviations.

### Applicability and Institutional Readiness

Vehicle compatibility varies. In vehicles where selective acquisition and masking functions are limited, policy/procedure-based compensation mechanisms have been designed. Education and awareness have played critical roles, especially in the correct operation of masking and consent flows. Periodic monitoring of process metrics (time of completion, number of access requests, mask opening rate, number of returns) has made areas of improvement visible.

### Sample Scenario (Corporate Internal Investigation)

Endpoint images were collected in an institutional internal investigation. With the ethical compliance matrix, only logs, business correspondence and files belonging to a certain period related to the incident are labeled as "necessary". Personal photos and private folders are classified as "unnecessary" or "conditionally necessary". Selective acquisition profiles were applied according to this classification; Special folders have been excluded from the process with masking. Analyst powers are limited to time; extension requests were managed with reasoned approval. During the reporting phase, chained audit records have strengthened defensibility by documenting all access and decision points. As a result, while the scope of evidence is preserved, unnecessary personal data exposure is reduced; the balance of review time and workload has improved.

## IV. DISCUSSION

### Strengths

The proposed approach brings TRIZ's contradiction-oriented thinking to forensic processes and balances the tensions of confidentiality-accessibility and speed-appropriateness with the principles of decomposition, selectivity, dynamism and retrievability. While ethical principles are transformed into concrete process and policy designs, auditability becomes a structural component in the process. The standard and record-oriented approach supports cross-agency benchmarking and improvement cycles.

### Limitations and Validity Threats

- **Quantitative validation:** Comparative measures and statistical analyses are required for different types of cases.
- **Tool dependency:** Selective acquisition/masking support may vary from tool; tool constraints can overburden process design.

- **Change management:** Approval flows, enrollment density, and role descriptions may conflict with internal habits; training and governance support is essential.

### Comparative Evaluation

Traditional broad acquisition and limited registration practices, while capable of providing speed, may lead to unnecessary personal data processing and vulnerabilities. The proposed framework focuses on balancing ethical and technical risks, considering data minimization and auditability simultaneously. Designs that align with process and recording standards ensure more consistent results and higher reliability in external auditing.

### Adaptability and Generalization

The framework can be adapted to different organizational scales and case types. The basic principle is to clearly name the contradictions and map them to the appropriate TRIZ principles; then to configure the solution components within the framework of institutional resources/constraints. It can be applied in contexts such as disk imaging, mobile analytics, log inspection, network forensics, and cloud resource inspections.

### Process Maturity and Compliance with Standards

As process maturity increases; the scope of registration, the quality of the decision justification and role/authority governance also mature. Compliance with institutional standards and external reference frameworks; It should be strengthened by monitoring through measurable metrics and independent review at certain periods. A continuous improvement approach ensures that feedback is translated into process and tool enhancements.

## V. CONCLUSION

This study systematically addressed the basic contradictions regarding personal data ethics in forensic informatics with the TRIZ approach and proposed practical solution components. Targeted acquisition and masking, ethical compliance matrix, evidence quarantine and auditable access, time-limited and revocable authorization, and chained audit-oriented registration mechanisms; Data minimization contributes to balancing evidence integrity, auditability, and operational efficiency.

**Major contributions:**

- Visibility of ethical tensions and contradiction-based solution generation.
- Transforming ethical principles into concrete process and policy designs.
- Positioning auditability as a standard component in the process.

**Future Studies:**

- Quantitative evaluations according to case types and measurement of process metrics (time of completion, number of access requests, mask opening rate, etc.).
- Tool integrations and automation: Expanding tool support for selective acquisition, masking, and audit trails.
- Institutional dissemination and training: Hands-on programs on role-based authorization models, ethical decision rationale writing, and enrollment standardization.

## REFERENCES


1. DFPulse: The 2024 Digital Forensic Practitioner Survey. *ScienceDirect*. Access: https://www.sciencedirect.com/science/article/pii/S2666281724001719
2. Mbimbi, B., Murray, D., & Wilson, M. (2024). IoT Forensics-Based on the Integration of a Permissioned Blockchain Network. *ResearchGate*. Access: https://www.researchgate.net/publication/259332114_Internet_of_Things_Forensics_Challenges_and_Approaches
3. Alenezi, A. M. (2023). Challenges in digital forensics for the Internet of Things. *Cybersecurity*. Access: https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/challenges-in-digital-forensics-for-the-internet-of-things/
4. Ashawa, M. A., Mansour, A., & Owoh, N. P. (2023). Digital forensics challenges in cyberspace: overcoming legitimacy and privacy issues through modularisation. *CCDS*. Access: https://ojs.wiserpub.com/index.php/CCDS/article/view/3845
5. Fahdi, M., & Clarke, N. L. (2023). Challenges to digital forensics: A survey of researchers. *Semantic Scholar*. Access: https://www.semanticscholar.org/paper/Challenges-to-digital-forensics%3A-A-survey-of-%26-and-Fahdi-Clarke/a5458578ef017357f4b81752e72d80d9d27bc794