DOI https://doi.org/10.32782/2956-333X/2026-6-6

ETHICAL DILEMMAS IN THE PROTECTION OF SOFT TARGETS

David Mazák,
PhDr. Ed.D., MBA
DTI Dubnica nad Váhom
https://orcid.org/0009-0008-5789-5622
mail@mazdav.cz

Summary. This study examines the ethical dilemmas associated with the protection of soft targets within the contemporary European security environment. It seeks to analyse the value conflicts arising from the implementation of modern security measures in publicly accessible spaces, particularly those involving surveillance technologies, biometric systems, and artificial intelligence. The study further aims to develop an analytical framework for assessing the legitimacy of protective measures by integrating security management, the European legal framework, and applied ethics. The study is based on a qualitative research design employing content analysis of scholarly literature, European strategic documents, European Union legislation, and the relevant case law of the Court of Justice of the European Union and the European Court of Human Rights. The analysis applies a normative ethical approach to evaluate conflicts between security requirements and the protection of fundamental rights within the European regulatory framework. The findings demonstrate that the principal ethical dilemmas of soft target protection arise from balancing public security with the protection of privacy, non-discrimination, transparency of decision-making, accountability in the use of artificial intelligence, and the preservation of public trust. The study proposes the Integrated Model of the Ethical Legitimacy of Soft Target Protection (IMEL–STP), which conceptualises legitimacy through three mutually dependent dimensions: security effectiveness, legal legitimacy, and ethical acceptability. The proposed model provides a systematic methodological framework for assessing the legitimacy of security measures that extends beyond traditional evaluations based solely on technical effectiveness or legal compliance. By integrating security studies, European law, and applied ethics, the model offers practical guidance for public authorities, security agencies, and operators of publicly accessible spaces while establishing a conceptual basis for future empirical research on the ethical legitimacy of soft target protection.

Keywords: soft target protection, ethics, security management, ethical legitimacy, proportionality, fundamental rights, artificial intelligence, AI Act, European regulatory framework, public trust.

1. Context of Soft Target Protection in the European Security Environment

The protection of soft targets represents one of the most significant areas of development in security policy and crisis management within the contemporary European security environment. The dynamic evolution of security threats, particularly attacks directed against publicly accessible spaces, has led the security community over the past two decades to fundamentally reassess approaches to the protection of the population and public spaces (European Commission, 2017). At the same time, it has become evident that traditional technical and security-oriented approaches are no longer sufficient on their own, as the protection of soft targets extends into the domains of fundamental rights, public administration, and democratic values.

A distinctive characteristic of soft targets is that their vulnerability is determined not only by a limited level of physical protection but, above all, by their societal function. Public spaces, transport hubs, schools, healthcare facilities, cultural institutions, and places of religious significance fulfil an irreplaceable role in the exercise of fundamental civil rights, freedom of movement, social interaction, and democratic participation. Their openness and accessibility constitute one of the fundamental values of European society while simultaneously increasing their attractiveness as potential targets of violent attacks (Karlos, Larcher and Solomos, 2018).

Within the European security discourse, this gives rise to a fundamental normative paradox. Measures adopted to protect an open society may, if inadequately designed, simultaneously contribute to the gradual erosion of the very values they are intended to protect. The extensive deployment of surveillance systems, biometric technologies, algorithmic tools, control regimes, and physical barriers may enhance the capability to prevent security incidents; however, it also interferes with individual privacy, alters the character of public space, affects perceptions of personal freedom, and may undermine public trust in the legitimacy of public authorities (European Commission, 2017; Council of Europe, 2021; EDPB, 2023).

Consequently, the protection of soft targets no longer represents merely a technical or organisational issue of security management. It is increasingly becoming a question of the legitimacy of public decision-making, requiring the balancing of security interests with the protection of fundamental rights, human dignity, equal treatment, and the preservation of the open character of public space. European institutions have consistently emphasized that security cannot be regarded as an absolute value but rather as a legitimate public interest that must be pursued in accordance with the principles of legality, necessity, and proportionality (European Union, 2012; European Commission, 2017).

The principle of proportionality constitutes one of the principal points of convergence between security management, European law, and applied ethics. Decisions concerning protective measures can no longer be reduced to questions of their technical effectiveness or economic efficiency. Every security measure simultaneously represents a value-based decision whose legitimacy depends not only on its ability to reduce risks but also on the extent to which it respects fundamental rights, ensures transparency of the decision-making process, defines the accountability of the actors involved, and secures societal acceptance of the measures adopted (Omand, 2010; Big Brother Watch and Others v. the United Kingdom, 2021).

Within this context, the protection of soft targets has become one of the most significant fields of applied security ethics. Ethical dilemmas therefore do not arise as a consequence of failures in security policy but rather constitute an inherent component thereof. Virtually every decision concerning the scope of protective measures requires the pursuit of a balance between legitimate yet frequently competing values. It is precisely this reality that creates the need for a systematic analysis of ethical dilemmas and their positioning within the contemporary European regulatory and judicial framework.

1.1 Methodological Approach

Although the protection of soft targets has become an important topic of European security policy in recent years, the scholarly literature has thus far focused primarily on the technical, organisational, and legal aspects of their protection. The predominant body of research addresses the analysis of terrorist threats, the assessment of the vulnerability of public spaces, risk management, and the design of physical and technological security measures (European Commission, 2019; Karlos, Larcher and Solomos, 2018; Kotková, 2021). By contrast, the systematic reflection on the ethical aspects of soft target protection remains relatively fragmented and is generally incorporated only as a subsidiary component of legal or security analyses.

A significant impetus for the development of this debate has been the rapid expansion of advanced surveillance technologies, biometric systems, and artificial intelligence-based tools. These technologies fundamentally transform the possibilities for preventing security threats while simultaneously raising new questions concerning the protection of privacy, the prohibition of discrimination, transparency of decision-making, human autonomy, and institutional accountability. Consequently, European regulatory policy increasingly links security requirements with the protection of fundamental rights, a development reflected not only in the general framework for personal data protection but also in the new regulation governing artificial intelligence systems (European Union, 2016; EDPB, 2023; European Union, 2024).

Despite these developments, there is still no comprehensive analytical approach that would enable the protection of soft targets to be assessed simultaneously in terms of security effectiveness, legal legitimacy, and ethical acceptability. The security literature generally emphasises risk management and the effectiveness of protective measures, whereas legal scholarship primarily focuses on the interpretation of individual regulatory instruments. Ethical issues tend to be discussed in isolation, without their systematic integration into security management and the European legal framework.

1.2 Objectives of the Article

The objective of this article is to analyse the ethical dilemmas associated with the protection of soft targets within the European security environment and, simultaneously, to develop an analytical framework integrating security management, the European regulatory framework, and applied ethics in assessing the legitimacy of protective measures. Particular attention is devoted to identifying value conflicts arising from the deployment of contemporary security technologies and to examining the role of European law as the normative framework for addressing these conflicts.

This objective is reflected in the following principal research question:

– What ethical dilemmas arise in the protection of soft targets within the European security environment, and how does the European regulatory framework contribute to their resolution?

– This principal question is complemented by two subsidiary research questions:

– What value conflicts arise from the application of contemporary security measures in publicly accessible spaces?

– Which principles of European law constitute the decisive criteria for assessing their ethical legitimacy?

Methodologically, the article is based on a qualitative research design employing content analysis of scholarly literature, European strategic documents, regulatory instruments, and the case law of the European Court of Human Rights and the Court of Justice of the European Union. The analytical part is grounded in the principles of normative ethical analysis, which enables the systematic evaluation of conflicts between security requirements and the protection of fundamental rights. The interdisciplinary approach adopted makes it possible to integrate insights from security studies, legal scholarship, and applied ethics into a coherent interpretative framework.

The contribution of this article lies not only in synthesising existing knowledge but, above all, in integrating that knowledge into a unified analytical framework that enables the legitimacy of soft target protection to be assessed not solely according to the security effectiveness of individual measures but also according to their compliance with the principles of proportionality, the protection of fundamental rights, transparency, and institutional accountability.

2. The Concept and Definition of Soft Targets

The concept of soft targets represents one of the key categories in contemporary security studies for analyzing current security threats. Existing definitions emphasise various characteristics, ranging from the physical vulnerability of facilities and the high concentration of people to their symbolic, economic, or societal significance (European Commission, 2017; Karlos, Larcher and Solomos, 2018).

Such definitions, however, capture only their security dimension. Equally important is their societal dimension. Soft targets comprise spaces in which everyday social life, education, culture, commerce, transportation, religious activities, and the exercise of fundamental civil rights take place. It is precisely this societal function that makes their protection particularly sensitive from the perspective of preserving democratic values.

A significant advancement in the conceptualization of soft targets is represented by an operationalised definition that combines the probability of an attack with its anticipated consequences, particularly in terms of potential loss of human life. This approach constitutes an important methodological shift, as it makes it possible to move beyond static categorizations of facilities and instead focus on the assessment of the actual level of risk. At the same time, it provides an appropriate basis for evaluating the proportionality of security measures, as it enables the intensity of interference with fundamental rights to be related to objectively identified security risks (Kotková, 2021).

2.1 Typology of Soft Targets and Its Significance for Ethical Analysis

Soft targets do not constitute a homogeneous category of facilities or public spaces. Individual types of soft targets differ considerably with respect to their societal function, operational characteristics, concentration of people, level of risk, and the possibilities for implementing security measures. This heterogeneity is one of the principal reasons why the protection of soft targets cannot be based on universal security procedures. Consequently, European methodological documents emphasise the need for a context-sensitive approach, which takes into account the specific characteristics of each protected space (Karlos, Larcher and Solomos, 2018).

In European security practice, soft targets most commonly include public spaces, shopping and cultural centers, educational and healthcare facilities, places of religious significance, and temporary mass events such as concerts, sporting events, markets, or public gatherings (European Commission, 2017; Karlos, Larcher and Solomos, 2018). Although all these environments are characterised by increased vulnerability to violent attacks, their protection requires different security strategies as well as different assessments of their impact on fundamental rights. For example, in the case of public parks, city squares,

or pedestrian zones, highly intensive security measures may significantly alter the character of public space and undermine its openness, which constitutes one of the fundamental values of a democratic society (European Commission, 2017).

Similarly, distinct ethical issues arise in relation to educational institutions, healthcare facilities, and places of worship. In schools, it is necessary to take into account the protection of minors, the autonomy of the educational environment, and the psychological effects of security measures. In healthcare facilities, respect must be given to human dignity, patient privacy, and the specific conditions under which healthcare services are provided. The protection of religious sites encompasses not only physical security but also the safeguarding of freedom of religion and the preservation of the symbolic significance of these places.

Accordingly, the scope and form of security measures should not be determined solely by the level of identified risk but must also reflect the societal function of the protected space, the nature of the rights exercised therein, and the legitimate expectations of its users.

Fig. 1. Classification of Security Measures for Soft Targets

Source: Author.

Based on the foregoing analysis, a general principle may be formulated: the more significant the societal function of a particular public space with respect to the exercise of fundamental rights and freedoms, the more stringent the requirements for the justification, proportionality, and transparency of the security measures adopted.

2.2 Soft Targets versus Critical Infrastructure

In both the academic literature and security practice, soft targets and critical infrastructure are sometimes discussed within the same context, although they represent two distinct categories of protected assets. While both are important to society, they differ with respect to the purpose of protection, legal status, nature of risks, and the possibilities for implementing security measures. Distinguishing between these categories is therefore not merely a terminological issue but is of fundamental importance for assessing the legitimacy of individual protective measures.

Critical infrastructure is defined by legal regulations as a set of systems, facilities, and services whose disruption would have serious consequences for national security, the economy, public administration, or the provision of essential services to the population. Its protection is based on a high degree of regulation, standardised security requirements, and clearly defined responsibilities of operators and public authorities. In these cases, a greater degree of security restrictions is generally accepted by society because the protected interest is the continuity of the functioning of the state and society.

By contrast, soft targets are spaces whose primary function is not the provision of critical services but rather the facilitation of ordinary social life. Their value lies precisely in their openness, accessibility, and the possibility of free movement. For this reason, security standards developed for critical infrastructure cannot simply be transferred to the protection of soft targets. Measures that are entirely legitimate

within a power plant, data centre, or water treatment facility may prove disproportionate when applied to a university, healthcare institution, or cultural venue (Karlos, Larcher and Solomos, 2018).

The distinction between the two categories becomes most evident when assessing the proportionality of protective measures. In the context of critical infrastructure, the decisive criterion is typically the minimization of the risk of operational disruption. In the protection of soft targets, however, security effectiveness must be evaluated alongside the impact of protective measures on the exercise of fundamental rights, the quality of public space, public trust, and the societal acceptability of the restrictions imposed. Consequently, the protection of soft targets is characterised by a substantially more complex process of balancing security interests against broader societal values (European Union, 2012; European Commission, 2017).

Another important difference concerns the institutional framework for protection. Critical infrastructure is governed by relatively clear rules regarding security management and accountability. In contrast, the protection of soft targets represents a typical example of multi-level governance, involving public authorities, law enforcement agencies, regional and local governments, facility operators, private security providers, and the public itself. This plurality of actors increases the demands placed on coordination, transparency of decision-making processes, and the clear allocation of responsibility for the measures adopted.

From the perspective of ethical analysis, this comparison leads to an important conclusion. Whereas the protection of critical infrastructure is based primarily on the principle of functional continuity, the protection of soft targets must be grounded in the principle of legitimate proportionality. Consequently, the success of protective measures cannot be evaluated solely by the absence of security incidents but also by whether the measures preserve the openness of public space, respect fundamental rights, and strengthen public trust in security institutions. It is precisely this characteristic that distinguishes the protection of soft targets from most other areas of security management and makes it a distinctive subject of applied ethics.

3. Ethical Dilemmas in the Protection of Soft Targets within the European Normative Framework

The protection of soft targets constitutes a specific area of security management in which several simultaneously legitimate public values come into conflict. On the one hand, the State has a positive obligation to ensure the protection of life, health, and public security; on the other hand, it is required to respect the fundamental rights of individuals, particularly the rights to privacy, freedom of movement, non-discrimination, and human dignity. Ethical dilemmas therefore do not arise as a consequence of inadequately designed security policies but represent the natural outcome of conflicts between values that a democratic state governed by the rule of law seeks to protect simultaneously (European Union, 2012).

For this reason, individual protective measures cannot be assessed solely on the basis of their security effectiveness. Equally important evaluation criteria include their legality, proportionality, transparency, public accountability, and societal acceptance. The European normative framework is founded on the premise that security is not an absolute value that automatically prevails over other fundamental rights but rather a legitimate public interest whose pursuit must always be proportionate to the objective pursued (European Union, 2012; European Commission, 2017).

The principle of proportionality constitutes the central methodological criterion for addressing ethical dilemmas in the protection of soft targets. Every security measure must not only be capable of achieving its intended objective but must also be necessary and proportionate in relation to the extent of the interference with fundamental rights. This approach has been consistently developed through the case law of both the Court of Justice of the European Union and the European Court of Human Rights and is likewise reflected in the current European regulatory framework governing personal data protection and artificial intelligence systems (Digital Rights Ireland, 2014; Big Brother Watch and Others v. the United Kingdom, 2021; European Union, 2024).

Based on the analysis conducted, several principal areas can be identified in which ethical conflicts arising from the protection of soft targets are most apparent. These include, in particular, the conflict between security and the right to privacy, the risk of discriminatory effects associated with certain security

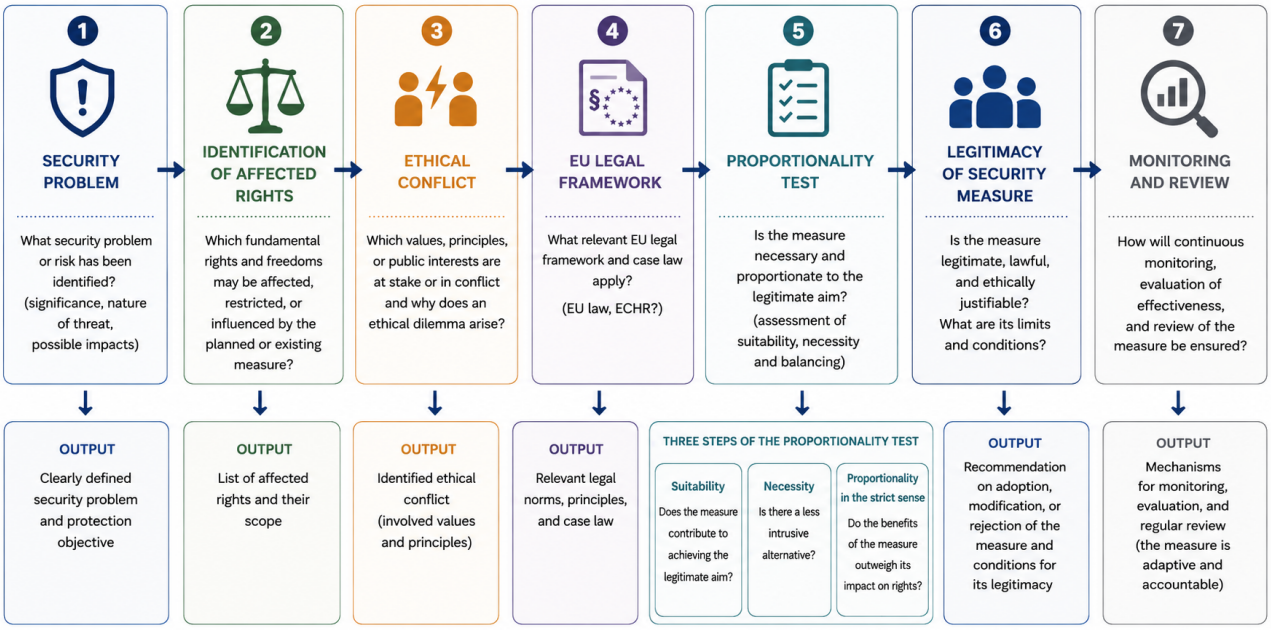

Fig. 2. Analytical Framework for Assessing Ethical Dilemmas in the Protection of Soft Targets

Source: Author.

technologies, issues relating to transparency and accountability in the use of artificial intelligence systems, and the question of public trust in the legitimacy of security measures. Although these conflicts differ in nature, they are all united by the need to achieve an appropriate balance between the effective protection of society and the preservation of the values upon which a democratic state governed by the rule of law is founded.

3.1 Security versus the Protection of Privacy

The conflict between the requirement to ensure security and the protection of privacy represents one of the most significant ethical dilemmas of contemporary security management. The development of surveillance technologies, CCTV systems, biometric identification, and artificial intelligence-based tools has substantially expanded the possibilities for preventing, detecting, and responding to security incidents. At the same time, however, these technologies enable the systematic collection, integration, and analysis of data concerning individuals' movements, behaviour, and identities within public spaces. Consequently, the protection of soft targets has become an area in which the legitimate public interest in ensuring security intersects with the individual's right to privacy (European Union, 2016; European Commission, 2017).

From an ethical perspective, the essence of this conflict does not lie in the existence of security technologies themselves but rather in the manner in which they are employed. CCTV systems, automated suspicious behaviour detection, and biometric identification technologies may make a substantial contribution to reducing security risks; however, their legitimacy depends upon the scope of surveillance, the purpose of data processing, the transparency of their use, and the existence of effective oversight mechanisms. The decisive question is therefore not whether such technologies should be employed but under what conditions their use may be regarded as proportionate and socially acceptable (Floridi et al., 2018; EDPB, 2023). Accordingly, every limitation of the right to privacy must satisfy the requirements of legality, legitimacy, necessity, and proportionality. These principles are enshrined both in the Charter of Fundamental Rights of the European Union and in the General Data Protection Regulation (GDPR) and have been consistently developed through the jurisprudence of the Court of Justice of the European Union and the European Court of Human Rights (European Union, 2012; European Union, 2016).

A landmark precedent in this regard was established by the judgment of the Court of Justice of the European Union in Digital Rights Ireland, which emphasized that the indiscriminate retention of information constitutes a disproportionate interference with fundamental rights unless it is limited to what is strictly

necessary and accompanied by appropriate procedural safeguards (Digital Rights Ireland, 2014). Similarly, in Big Brother Watch and Others v. the United Kingdom, the European Court of Human Rights held that even serious security threats do not justify the uncontrolled use of mass surveillance systems in the absence of adequate legal safeguards, independent oversight, and effective mechanisms for the protection of individual rights (Big Brother Watch and Others v. the United Kingdom, 2021).

These conclusions are directly relevant to the protection of soft targets. Publicly accessible spaces represent environments in which security technologies interact most intensively with the exercise of fundamental rights. Decisions concerning the scope of CCTV surveillance, the use of biometric identification, or the implementation of artificial intelligence systems cannot therefore be based exclusively on the technical capabilities of these tools. An indispensable component of the decision-making process must be an assessment of their impact on fundamental rights, public expectations, and the long-term trust of citizens in public institutions (OECD, 2019).

From the perspective of applied ethics, it is therefore possible to formulate the general principle that the legitimacy of security technologies is derived not solely from their effectiveness but from their ability simultaneously to satisfy the requirements of security effectiveness, legal legality, and ethical proportionality. Without due regard to all three dimensions, the protection of soft targets cannot be regarded as either sustainably legitimate or socially acceptable.

3.2 Security versus Equal Treatment and the Prohibition of Discrimination

Alongside the protection of privacy, one of the most significant ethical dilemmas in the protection of soft targets concerns the risk of discriminatory effects arising from security measures. This risk has become increasingly prominent in recent years with the expanding use of artificial intelligence systems, biometric identification, behavioural analysis, and predictive security tools. Although these technologies are developed with the objective of enhancing the effectiveness of preventing and detecting security threats, their practical application may result in unequal treatment of individuals or groups based on ethnic origin, nationality, age, sex, religion, or other protected characteristics (Floridi et al., 2018; European Union, 2024).

From an ethical perspective, the problem does not lie solely in intentional discrimination. A substantial proportion of contemporary risks arises from indirect discrimination resulting from the configuration of algorithms, the quality of training data, or the manner in which security systems are implemented. Automated decision-making processes may reproduce existing societal inequalities or generate new forms of systemic disadvantage without such outcomes being intentionally pursued. Accordingly, applied ethics requires an assessment not only of the technical accuracy of an algorithm but also of the fairness of its outcomes and their impact on both individuals and social groups (Mittelstadt et al., 2016; Dignum, 2019).

A specific characteristic of soft target protection is that security measures are generally implemented within publicly accessible spaces where they affect highly diverse populations. Although intensified security controls directed towards particular groups may increase the short-term effectiveness of protective measures, they may simultaneously contribute to the stigmatization of communities, undermine public trust in security institutions, and reduce citizens' willingness to cooperate in preventing security threats. Long-term security therefore depends not only on the effectiveness of coercive measures but also on maintaining the legitimacy of public authorities and public confidence in their impartiality.

The European normative framework addresses these risks through the principles of non-discrimination, the protection of human dignity, and the requirement for human oversight of automated decision-making. In this regard, particular importance is attached to the Artificial Intelligence Act (AI Act), which classifies certain biometric identification and remote biometric recognition systems as high-risk applications and imposes stringent requirements concerning risk management, data quality, transparency, human oversight, and technical documentation (European Union, 2024). These requirements do not merely constitute technical regulation of artificial intelligence systems but also express the normative commitment to preserving fair and non-discriminatory decision-making.

The case law of the European Court of Human Rights has consistently emphasised that differential treatment of individuals may be justified only where it pursues a legitimate aim and is objectively and proportionately justified. In the context of soft target protection, this means that security measures must not

be based on stereotypical assumptions regarding the risk posed by particular population groups but rather on concrete, objective, and verifiable security information. Consequently, the decision-making process must be not only effective but also transparent and subject to review.

From the perspective of security management, this analysis leads to an important conclusion. The effectiveness of security measures cannot be evaluated solely according to their capacity to identify potential threats but must also be assessed according to their ability to preserve equal treatment, minimize the risk of discriminatory effects, and strengthen public confidence. A security system that persistently undermines social cohesion or creates perceptions of unjust treatment may, paradoxically, contribute to the emergence of new security risks. The ethical legitimacy of soft target protection is therefore inseparably linked to the principles of equality, fairness, and respect for human dignity.

3.3 Transparency, Accountability, and the Use of Artificial Intelligence

The increasing deployment of artificial intelligence systems represents one of the most significant transformations in contemporary security management. Technologies based on machine learning and advanced data analytics enable the automated processing of vast quantities of information, the identification of anomalous patterns of behaviour, and decision support in the protection of publicly accessible spaces. Their principal benefits include faster information processing, more effective detection of security incidents, and more efficient utilisation of the limited human resources available to security authorities. At the same time, however, these technologies fundamentally alter the nature of security decision-making and give rise to new ethical and legal challenges (Floridi, 2023; Dignum, 2019).

Unlike traditional security technologies, artificial intelligence systems are no longer confined to the operational implementation of security measures but increasingly influence the decision-making process itself. Algorithms may recommend the deployment of security resources, identify individuals or situations assessed as presenting elevated risk, analyse visual data obtained from surveillance systems, or support predictive analyses of security threats. Although the final decision generally remains within the competence of a human decision-maker, increasing reliance on algorithmic recommendations may diminish critical evaluation of system outputs and give rise to the phenomenon known as automation bias, namely an unwarranted degree of confidence in automated systems (Parasuraman and Manzey, 2010).

From an ethical perspective, one of the principal concerns relates to the limited transparency of certain artificial intelligence systems. In the case of advanced machine-learning models, it is often difficult to explain retrospectively which input data and decision-making rules led the algorithm to a particular conclusion. The limited explainability of algorithmic decision-making complicates independent review, weakens the accountability of the actors involved, and may reduce public confidence in the legitimacy of security measures. Transparency should therefore not be regarded merely as a technical characteristic of an information system but rather as one of the fundamental prerequisites for the responsible exercise of public authority (Floridi et al., 2018; Mittelstadt et al., 2016).

These challenges are addressed within the European normative framework through the Artificial Intelligence Act (AI Act), which establishes a risk-based approach to the regulation of artificial intelligence systems. AI systems deployed in law enforcement and public security are, under certain conditions, classified as high-risk systems and are therefore subject to stringent requirements concerning risk management, data quality, technical documentation, transparency, human oversight, and continuous monitoring of their operation (European Union, 2024). The objective of this regulatory framework is not to impede technological innovation but to ensure that the deployment of artificial intelligence remains compatible with the protection of fundamental rights and the principles of a democratic state governed by the rule of law.

A key principle underpinning the European approach is the requirement for meaningful human oversight. Decisions having significant implications for the fundamental rights of individuals must not be delegated exclusively to automated systems. Artificial intelligence should support, rather than replace, human decision-making. Responsibility for the security measures adopted therefore continues to rest with the competent public authority or other responsible entity, which must be capable of providing reasons for its decisions and of subjecting them to independent review.

In the context of soft target protection, it follows that the introduction of artificial intelligence systems cannot be assessed solely on the basis of their technical accuracy or economic efficiency. Equal attention

must be devoted to their transparency, explainability, reviewability, and the accountability associated with their use. Only when these conditions are fulfilled simultaneously can artificial intelligence systems contribute to enhancing security without undermining public trust or weakening the legitimacy of security decision-making.

3.4 Public Trust as a Prerequisite for the Legitimacy of Protective Measures

Although security measures are generally evaluated according to their ability to prevent security incidents or mitigate their consequences, the long-term effectiveness of soft target protection also depends on the level of public trust in the institutions responsible for their implementation. A security policy based exclusively on technical or coercive instruments may contribute to enhancing protection in the short term; however, without societal legitimacy and public confidence, its effectiveness will inevitably decline over time. Public trust should therefore be regarded not merely as a sociological or political phenomenon but also as a fundamental component of effective security management.

The importance of public trust is particularly evident in the context of soft targets, which are characterised by continuous interaction among citizens, facility operators, and public authorities. Unlike critical infrastructure, the protection of these environments cannot be ensured solely through physical barriers or control mechanisms. Equally important are the willingness of members of the public to comply with security measures, cooperate in preventing security risks, report suspicious activities, and accept proportionate restrictions on certain fundamental rights. Public trust thus becomes one of the essential prerequisites for the overall resilience of society to security threats.

From an ethical perspective, the significance of trust lies in the long-term legitimacy of public authority. Citizens are generally willing to accept even relatively intrusive security measures provided that they understand their purpose, perceive them as fair, and are confident that they are implemented in a transparent, non-discriminatory, and reviewable manner. Conversely, opaque decision-making processes, disproportionate use of surveillance technologies, or repeated instances of discrimination may erode public confidence, thereby diminishing the effectiveness of the security measures themselves.

Accordingly, contemporary European security policy increasingly emphasises the principles of good governance, public accountability, transparency of decision-making, and public participation. These principles are not merely general aspirations but constitute practical instruments for strengthening the legitimacy of security measures. Consequently, the protection of soft targets provides a clear example of an area in which security management naturally intersects with the principles of democratic governance and the protection of fundamental rights (European Commission, 2017; Council of Europe, 2021).

The importance of public trust becomes even greater with the increasing deployment of advanced digital technologies. Members of the public generally do not possess the technical expertise necessary to assess the functioning of algorithmic systems or biometric technologies. Their acceptance of such technologies therefore depends primarily upon confidence in the institutions deploying them, the quality of the applicable regulatory framework, and the existence of effective mechanisms of independent oversight. Transparent communication regarding the purpose, scope, and limitations of security technologies thus constitutes an essential precondition for their societal acceptance.

In the context of soft target protection, public trust should therefore not be regarded merely as a desirable by-product of security policy. Rather, it constitutes one of its fundamental prerequisites. Security measures that are technically effective but simultaneously undermine public confidence in public institutions may ultimately reduce society's overall resilience to security threats. The legitimacy of soft target protection therefore requires not only security effectiveness and legal compliance but also the capacity to sustain public trust through transparent, accountable, and proportionate decision-making.

3.5 An Integrated Model of the Ethical Legitimacy of Soft Target Protection

The foregoing analysis demonstrates that the ethical dilemmas associated with the protection of soft targets should not be understood as isolated problems arising from particular security technologies or individual legal instruments. Rather, they constitute interconnected manifestations of a broader conflict between the imperative of ensuring security and the protection of the fundamental values of a democratic state governed by the rule of law. The protection of privacy, the prohibition of discrimination, the transparency of algorithmic decision-making, public accountability, and public trust therefore do not represent

separate areas of ethical reflection but together form the normative framework within which the legitimacy of security measures must be assessed.

On the basis of the analysis conducted, it is possible to propose an Integrated Model of the Ethical Legitimacy of Soft Target Protection (IMEL–STP), which integrates three interdependent dimensions of decision-making:

a) security effectiveness;

b) legal legitimacy;

c) ethical acceptability.

These dimensions should not be understood hierarchically or as alternative decision-making criteria. Each represents an indispensable condition for the legitimate implementation of security policy, while the balance among them determines the overall acceptability of any particular protective measure.

The first dimension, security effectiveness, addresses the question of whether a proposed measure genuinely contributes to reducing an identified security risk. Assessment focuses primarily on the measure's capacity to prevent security incidents, the appropriateness of its technical design, and the existence of empirical evidence supporting its effectiveness. A measure that fails to provide a genuine improvement in security cannot be regarded as legitimate, irrespective of its legal or ethical acceptability.

The second dimension is legal legitimacy, which is derived from the requirement that security measures comply with constitutional principles, European Union law, and the international framework for the protection of human rights. Particular attention is devoted to the legality of the measure, compliance with the principle of proportionality, the protection of personal data, the availability of judicial review, and the existence of accountability for decisions taken. Legal legitimacy establishes the minimum standard of protection against arbitrary exercises of public authority.

The third dimension, ethical acceptability, extends beyond the legal framework by focusing on the broader societal consequences of security measures. Assessment within this dimension includes respect for human dignity, the preservation of equal treatment, the transparency of decision-making processes, the existence of meaningful human oversight in the use of advanced technologies, and the long-term impact of security measures on public trust. It is this dimension that ultimately determines whether security measures are perceived as legitimate not only from a legal perspective but also in light of democratic values.

The proposed model further demonstrates that these three dimensions are mutually interdependent. Improvements in security effectiveness must not be achieved at the expense of disproportionate restrictions on fundamental rights. Likewise, formal compliance with legal requirements does not necessarily guarantee the ethical acceptability of a particular measure. The sustainable protection of soft targets therefore requires the continuous balancing of all three dimensions and the regular reassessment of adopted measures in response to evolving security threats, technological developments, and changing societal expectations.

The Integrated Model of the Ethical Legitimacy of Soft Target Protection is not intended merely as a theoretical construct. It may serve as a methodological framework for decision-making by public authorities, law enforcement agencies, operators of publicly accessible facilities, and other entities responsible for the protection of soft targets. At the same time, it provides a systematic basis for assessing newly introduced security technologies, particularly those based on artificial intelligence, whose implementation is expected to constitute one of the principal challenges for European security policy in the coming years.

4. Conclusion

The protection of soft targets represents one of the areas in which the transformation of the contemporary concept of security is most clearly manifested. Traditional approaches based primarily on the physical protection of facilities and the management of security risks are no longer sufficient on their own. The rapid development of digital technologies, the increasing deployment of artificial intelligence systems, and the growing emphasis on the protection of fundamental rights have created an environment in which security measures must be assessed not only in terms of their technical effectiveness but also with regard to their legal and ethical legitimacy.

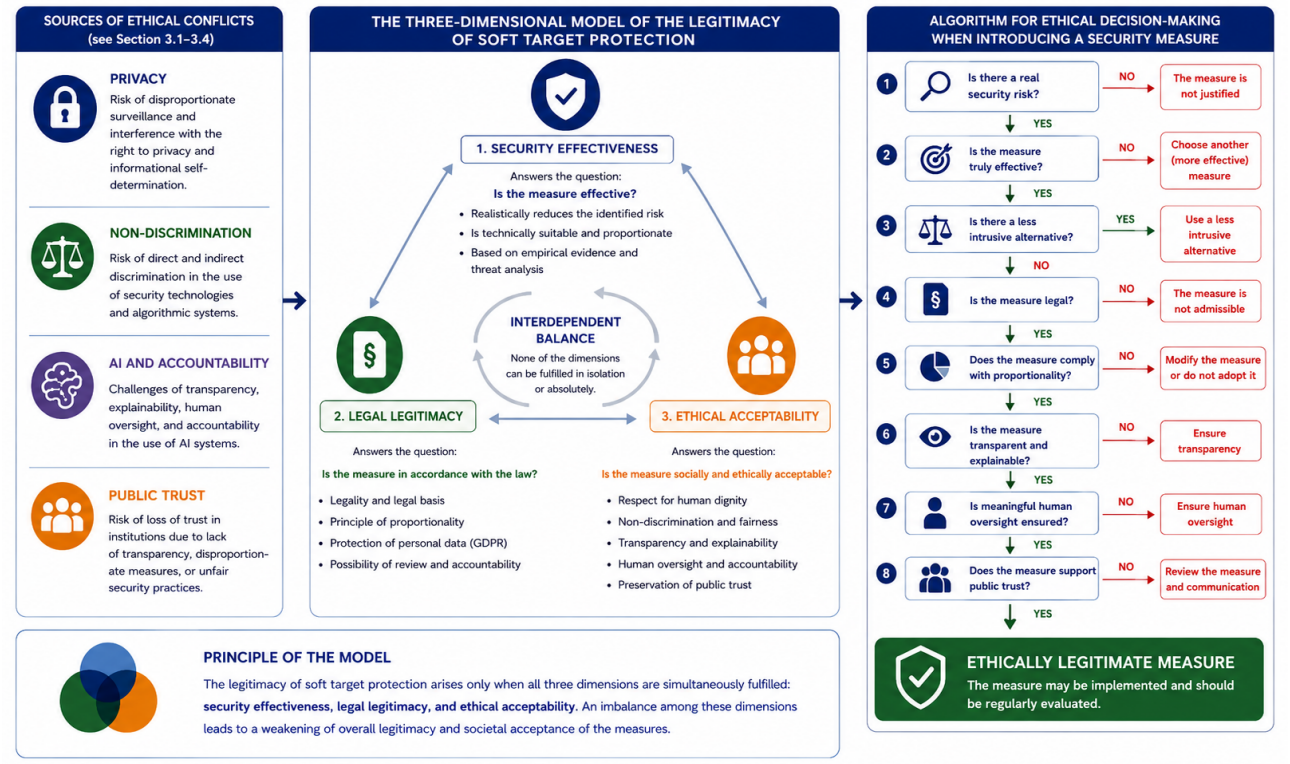

Fig. 3. Integrated Model of the Ethical Legitimacy of Soft Target Protection (IMEL–STP)

Source: Author.

The objective of this article was to analyze the ethical dilemmas associated with the protection of soft targets within the European security environment and to develop an analytical framework integrating insights from security management, the European normative framework, and applied ethics. The analysis has demonstrated that the most significant ethical conflicts arise in balancing the protection of life and public security against the protection of privacy, the prohibition of discrimination, the transparency of decision-making processes, the responsible use of artificial intelligence systems, and the preservation of public trust in the legitimacy of security measures.

The principal theoretical contribution of this article is the formulation of the Integrated Model of the Ethical Legitimacy of Soft Target Protection (IMEL–STP). The model is founded on the premise that the legitimacy of security measures cannot be derived solely from their capacity to reduce security risks or from their compliance with applicable legal requirements. Legitimate protection of soft targets exists only where three mutually interconnected dimensions of decision-making are simultaneously fulfilled: security effectiveness, legal legitimacy, and ethical acceptability. The model therefore provides a systematic framework for evaluating security measures that transcends the traditional separation of technical, legal, and ethical aspects of the protection of publicly accessible spaces.

The proposed analytical framework may serve as methodological guidance for public authorities, law enforcement agencies, operators of publicly accessible facilities, and other entities responsible for the protection of soft targets. It is particularly applicable to the design and evaluation of security measures employing CCTV systems, biometric identification technologies, or artificial intelligence-based tools, the implementation of which will increasingly be shaped by the European regulatory framework, particularly the Artificial Intelligence Act (AI Act).

The present study is, however, subject to certain limitations. It is based on a qualitative analysis of scholarly literature, European strategic documents, legal instruments, and relevant case law. Future research should therefore focus primarily on the empirical validation of the proposed model within the contexts of public administration and security practice, on analyzing the implications of the implementation of the Artificial Intelligence Act for the protection of soft targets, and on further developing methods for

assessing public trust as one of the key indicators of the legitimacy of security measures. An additional challenge will be the development of methodologies capable of continuously evaluating the proportionality of security measures in an environment characterised by rapidly evolving digital technologies.

It may therefore be concluded that the protection of soft targets can no longer be regarded merely as a matter of security management or the technical protection of publicly accessible spaces. Rather, it has become a complex process of public decision-making in which security, legal, technological, and ethical considerations intersect. The long-term sustainability of soft target protection will therefore depend not only on the sophistication of the technologies employed or the scope of the security measures adopted but, above all, on the ability of democratic societies to maintain an appropriate balance between safeguarding security and preserving the fundamental values that security policy is intended to protect.

Bibliography

1. Big Brother Watch and Others v. the United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, Judgment of the European Court of Human Rights, 25 May 2021.
2. Council of Europe. (2021). Guidelines on Facial Recognition. Strasbourg: Council of Europe.
3. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12, Judgment of the Court of Justice of the European Union, 8 April 2014.
4. Dignum, V. (2019). Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way. Cham: Springer.
5. European Commission. (2017). Action Plan to Support the Protection of Public Spaces. Brussels: European Commission.
6. European Commission. (2017). Commission Staff Working Document on the Protection of Public Spaces. Brussels: European Commission.
7. European Data Protection Board. (2023). Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement. Brussels: EDPB.
8. European Union. (2012). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*, C326, 391–407.
9. European Union. (2016). 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*, L119, 1–88.
10. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L, 2024/1689.
11. Floridi, L. (2023). The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. DOI: 10.1093/oso/9780198883098.001.0001.
12. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P. and Vayena, E. (2018). AI4People – An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707.
13. Karlos, V., Larcher, M. and Solomos, G. (2018). Soft Target Protection: Best Practices to Enhance the Security of Buildings. Luxembourg: Publications Office of the European Union.
14. Kotková, D., Kotek, L., Jenčková, K., Kalvach, Z., Šternová, T. (2021). Hromadné společenské a kulturní akce a jejich ochrana. ISBN 978-80-7678-058-3
15. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2). DOI: 10.1177/2053951716679679.
16. OECD. (2019). OECD Principles on Artificial Intelligence. Paris: Organisation for Economic Co-operation and Development.
17. Omand, D. (2010). Securing the State. London: Hurst & Company.
18. Parasuraman, R. and Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors*, 52(3), 381–410. DOI: 10.1177/0018720810376055.