# KÖZIGAZGATÁSI ÉS INFOKOMMUNIKÁCIÓS JOGI PHD TANULMÁNYOK

# PHD STUDIES IN ADMINISTRATIVE AND ICT LAW

2025/III.

VI. évfolyam - Volume 6

# KÖZIGAZGATÁSI ÉS INFOKOMMUNIKÁCIÓS JOGI PHD TANULMÁNYOK

2025. évi III. SZÁM
VI. ÉVFOLYAM

HU – (e)ISSN: 2732-0731

Kiadó: Tudatosan a Környezetünkért Egyesület
Felelős kiadó: Dr. Hohmann Balázs, egyesületi elnök.



Cím: Tudatosan a Környezetünkért Egyesület
7630 Pécs, Deák Ferenc u. 126.
tudatosanpecs@gmail.com

# PHD STUDIES IN ADMINISTRATIVE AND ICT LAW

ISSUE III, 2025
VOLUME VI

HU – (e)ISSN: 2732-0731

Publisher: Tudatosan a Környezetünkért Egyesület (Consciously for Our Environment Association)

Responsible for publishing: Dr. Balázs Hohmann Ph.D., President of the Association



Address: Tudatosan a Környezetünkért Egyesület (Consciously for Our Environment Association)
Pécs (HU-7630)
126 Deák Ferenc Str.
tudatosanpecs@gmail.com

## FOREWORD

The latest issue of our journal places at its centre the dynamically evolving intersections of administrative law and ICT law. The studies address both the fundamental rights, regulatory and institutional questions raised by technological development, and the practical challenges that are becoming increasingly prominent in the fields of artificial intelligence, robotics, data protection, energy market supervision, and the protection of human rights in the digital environment.

The particular value of this issue lies in the fact that our authors do not merely analyse the applicable legal frameworks, but also examine their practical operation, comparative experiences, and possible future directions of development. Forensic robotics and integrated security systems, the mechanisms of the REMIT Regulation designed to safeguard energy market integrity, the impact of technological development on human rights, and the knowledge-oriented regulatory approaches of the GDPR and the AI Act all demonstrate that, for contemporary legal scholarship, digitalisation is no longer an external circumstance, but a factor that fundamentally shapes legal thinking.

On behalf of the Publisher, I would like to thank our Authors for their dedication, and the members of the Editorial Board and the reviewers for accepting our invitations and for their invaluable work. Special thanks are due to the colleagues of the South Transdanubian Regional Library and Knowledge Centre, whose support is indispensable for the publication of our journal.

I wish all readers a good professional "immersion"!

*Dr. Balázs Hohmann*
*Editor-in-Chief*

## ELŐSZÓ

Folyóiratunk legújabb száma a közigazgatási és infokommunikációs jog dinamikusan változó metszéspontjait állítja középpontba. A tanulmányok egyaránt foglalkoznak a technológiai fejlődés által felvetett alapjogi, szabályozási és intézményi kérdésekkel, valamint azokkal a gyakorlati kihívásokkal, amelyek a mesterséges intelligencia, a robotika, az adatvédelem, az energiapiaci felügyelet és a digitális környezetben érvényesülő emberi jogok területén mind hangsúlyosabbá válnak.

A lapszám különös értékét adja, hogy szerzőink nem csupán a hatályos jogi keretek elemzésére vállalkoznak, hanem azok gyakorlati működését, összehasonlító tapasztalatait és jövőbeli fejlesztési irányait is vizsgálják. A kriminalisztikai robotika és az integrált biztonsági rendszerek, a REMIT-rendelet energiapiaci integritást védő mechanizmusai, a technológiai fejlődés emberi jogokra gyakorolt hatásai, valamint a GDPR és az AI Act tudásorientált szabályozási megközelítései egyaránt azt mutatják, hogy a kortárs jogtudomány számára a digitalizáció már nem külső körülmény, hanem a jogi gondolkodást alapjaiban formáló tényező.

A Kiadó nevében ezúton is köszönöm Szerzőink igyekezetét, a Szerkesztőbizottság tagjainak és a lektoroknak a felkérések elfogadását és áldozatos munkájukat. Külön köszönet illeti a Dél-dunántúli Regionális Könyvtár és Tudásközpont munkatársait, akik sokoldalú szakmai és technikai támogatásukkal továbbra is nélkülözhetetlen segítséget nyújtanak folyóiratunk megjelentetéséhez.

Jó szakmai „merítkezést” kívánok minden Olvasónak!

*Dr. Hohmann Balázs*
*főszerkesztő*

# KÖZIGAZGATÁSI ÉS INFOKOMMUNIKÁCIÓS JOGI PHD TANULMÁNYOK
# PHD STUDIES IN ADMINISTRATIVE AND ICT LAW

2025. évi III. SZÁM
VI. ÉVFOLYAM

ISSUE III, 2025
VOLUME VI

**TARTALOM – TABLE OF CONTENTS**

# FROM AWARENESS TO LITERACY: KNOWLEDGE ORIENTATION IN THE REGULATORY ENVIRONMENT OF THE GDPR AND THE AI ACT

*Dr. Tamás Sándor Török*
*Doctorate student, Doctoral Shool of Law, University of Pécs (Hungary)*
*Corresponding address: tamas.drtorok@gmail.com*
*ORCID: 0009-0006-1065-1730*

**DOI: 10.47272/KIKPhD.2025.3.1**

**ABSTRACT**

The comparative analysis of the General Data Protection Regulation and the Artificial Intelligence Act has become one of the most prominent topics in contemporary legal scholarship. This is due to several reasons, one of the most important being that the impact of both instruments extends far beyond the European Union, allowing them to function as de facto global standards. At the same time, both legislative texts are products of the digital age, and consequently their interpretation and the demonstration of compliant behaviour require specific competencies and prior knowledge.

This study analyses the concept of "AI literacy" as defined in the Artificial Intelligence Act, drawing on the notion of "data protection awareness" under the General Data Protection Regulation and on empirical findings from available research data, with a view to mapping potential risks and challenges. Digital literacy, awareness, and literacy more broadly are concepts without which compliant behaviour in the field of technology regulation cannot realistically be expected. Accordingly, experience gained under the GDPR provides important lessons for the development of AI literacy as well.



**KEYWORDS**

GDPR awareness, AI literacy, AI Act, GDPR, digital literacy, data subject

**ARTICLE HISTORY**

SUBMITTED 14 Nov 2025 | REVISED 21 Nov 2025 | ACCEPTED 1 Dec 2025

## I. Introduction and Working Hypothesis

It is characteristic of technology regulation that it seeks to govern an environment which is subject to constant and dynamic change and which, at the same time, demands a high level of prior knowledge from both legal practitioners and other legal and natural persons. In order to anticipate the expected impact and effectiveness of such regulation, it is therefore necessary to understand and assess the relevant competencies of those persons subject to it, as their knowledge and skills directly influence regulatory effectiveness.

In the case of more recent European Union regulatory instruments, a knowledge-oriented approach can be observed alongside the now familiar risk-based approach, at least as regards data protection law and the emerging regulation of artificial intelligence.

The present study seeks to answer how the concepts of data protection awareness and artificial intelligence literacy relate to one another, how and from which perspectives they can be interpreted, and, in light of their different temporalities, which conclusions and lessons can be drawn from the practical experiences with data protection awareness for the regulation of artificial intelligence and, by extension, for future technology regulation more generally.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on artificial intelligence (hereinafter: Artificial Intelligence Act or AIA) aims to provide relevant responses to several key risks brought to the fore by AI technologies.[1] A central element of this regulatory strategy is the introduction of the concept of AI literacy and its elaboration as a normative category.



It is important to note, however, that the interpretation of "literacy" ipso facto extends beyond the boundaries of legal scholarship. Its definition necessarily involves, in addition to the analysis of the addressees of the regulation, questions of measurability and evaluability of outputs. This in turn requires drawing on other social sciences and, where appropriate, on pedagogical research in order to arrive at adequate conclusions.

The examination of AI literacy inevitably presupposes an analysis of the practical experiences accumulated in relation to "data protection awareness" under the General Data Protection Regulation. Data protection awareness, similarly to AI literacy, seeks to promote the preparedness of the "receiving side", and the research results generated in the seven years following the applicability of 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, repealing Directive 95/46/EC (hereinafter: GDPR

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on artificial intelligence, OJ L 2024/1689.

or General Data Protection Regulation), may thus provide relevant initial lessons for the AIA.[2]

The study therefore addresses the following central questions: what is the precise normative content of the concepts of data protection awareness and AI literacy, and which addressee groups do they burden with what types of responsibilities? The working hypothesis is that the foundations of data protection awareness and AI literacy can be aligned conceptually, and that legislative and practical experiences generated under the GDPR are consequently worth considering and, where appropriate, adapting in the context of the AIA as well.

## II. Framework of Data Protection Awareness

### *1. Complexity of Data Protection Awareness*

The General Data Protection Regulation has undoubtedly brought about far-reaching changes in the protection of personal data worldwide. In adopting the GDPR, the European Commission sought to achieve several declarative objectives, including increasing transparency for data subjects regarding the processing of their personal data, enhancing individuals' control over their own data, and promoting data protection awareness.[3]

In its Communication entitled "Data protection rules as a trust-enabler in the EU and beyond -- taking stock", the Commission characterised the EU data protection legal framework as "a cornerstone of the European, human-centric approach to innovation".[4] In the same document, the Commission acknowledged that, although individuals are increasingly aware of their rights and are exercising them more frequently, additional efforts are required in order to further raise awareness.



It is important to emphasise, however, that data protection awareness is a highly complex concept which is not defined in the normative text of the GDPR. As a result, several possible approaches exist for understanding its meaning. The GDPR explicitly assigns obligations related to data protection awareness to two actors: the data protection officer and the supervisory authorities.

The tasks of the data protection officer include ensuring "awareness-raising and training of staff involved in processing operations".[5] As regards supervisory authorities, the legislative text is more detailed. Recital 132 already states

[2] 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, repealing Directive 95/46/EC, OJ L 2016/679.

[3] European Commission, *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond -- taking stock* (2019) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0374.

[4] Ibid.

[5] Regulation (EU) 2016/679, art 39(1)(b).

that "[a]wareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons, in particular in the educational context".[6] In addition, the GDPR entrusts supervisory authorities with the task of educating the public by requiring them, in the framework of promoting "public awareness and understanding of the risks, rules, safeguards and rights in relation to processing", to inform not only controllers and processors but also natural persons.[7] Furthermore, supervisory authorities are obliged to draw the attention of controllers and processors to their obligations under the Regulation.

It is equally striking that the GDPR does not formulate explicit expectations with regard to awareness on the part of data subjects, nor does it set out any behavioural expectations in respect of data processing. Only Recital 47 refers to "the reasonable expectations of data subjects" as a benchmark in the context of legitimate interest.[8]

Data protection awareness is multi-component. One of its cornerstones is the concept of privacy itself, for which there is no single, universally accepted definition. From the perspective of the present study, only two approaches will be highlighted here. Paul A. Pavlou defines privacy as an individual's right to determine what personal information to share with others and under which circumstances.[9] Data or information confidentiality forms an integral part of privacy protection and, according to Luciano Floridi, "functions as a shield of personal identity".[10]

Understanding the position of natural persons -- or data subjects, in the terminology of the GDPR -- is a prerequisite for answering the research questions. While Article 8 of the Charter of Fundamental Rights of the European Union provides fundamental rights protection for personal data, there is no comparable, clearly articulated fundamental rights framework underpinning the AIA.[11]



Despite this difference in fundamental rights orientation, or precisely because of it, the protection of natural persons remains of crucial importance, as it provides the basis for the practical implementation of all subsequent provisions.

As a starting point, it is worth accepting that every individual is vulnerable. However, the degree and nature of individual vulnerability differ and depend on social contexts and relational structures.[12] According to Florencia Luna, the intensity

[6] Ibid, Recital 132.
[7] Ibid, art 57(1).
[8] Ibid, Recital 47.
[9] Paul A Pavlou, 'Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model' (2003) 7(3) *International Journal of Electronic Commerce* 101. https://doi.org/10.1080/10864415.2003.11044275
[10] Luciano Floridi, 'The Ontological Interpretation of Informational Privacy' (2005) 7(4) *Ethics and Information Technology* 129. https://doi.org/10.1007/s10676-006-0001-7
[11] See Regulation (EU) 2024/1689, Preamble (recitals 1-79) and arts 1-71, which do not contain an explicit fundamental rights framework comparable to that in the GDPR.
[12] Gianclaudio Malgieri and Jedrzej Niklas, 'Vulnerable data subjects' (2020) 37(1) *Computer Law & Security Review* 105482. https://doi.org/10.1016/j.clsr.2020.105415

of legal protection afforded to vulnerable persons must be proportionate to the quantity and quality of so-called layers of vulnerability. The identification and assessment of these layers must be based on multiple criteria, in particular on the analysis of the origin and effects of vulnerability.[13] Luna concludes that the obligations arising from the assessment of layers of vulnerability must extend to preventing their deterioration, eliminating them where possible, and minimising them through different strategies.[14]

Transposed into the context of data protection law, this raises the question of whether an individual or a universal approach to vulnerability should be preferred. According to the universal approach, data protection law protects all individuals equally in the digital sphere, as all natural persons are equally exposed to potential infringements.[15] The individual approach, by contrast, offers a more accurate picture of risks affecting specific persons, yet it is doubtful to what extent it can be effectively implemented in practice.

Closely related to this distinction is the observation that, due to the rigidity of the concept of "data subject",[16] the assessment of individual vulnerability may easily become generalised, with the result that protective measures adopted for data subjects risk becoming schematic and ineffective.

The GDPR itself supports this concern by distinguishing between "general" data subjects and, for example, children as a group requiring special protection. In this latter case, increased protection is justified, as children, due to their age, are less able to understand the circumstances and effects of specific processing operations, and their level of data protection awareness can therefore only be expected to be relatively low. Reference should also be made to the provisions on data protection impact assessments and the handling of data breaches, where the GDPR places the consideration of individual interests and preferences at the centre of the analysis. However, this recognition must lead to the conclusion that other social groups, due to their life circumstances, are likewise limited in their ability to exercise their rights. One only needs to think of illiteracy.[17]



The determination of vulnerability and of those groups that require special protection is particularly complex and urgent in the context of digital citizenship.

[13] Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers not Labels' (2009) 2(1) *International Journal of Feminist Approaches to Bioethics* https://doi.org/10.3138/ijfab.2.1.121

[14] Florencia Luna, 'Identifying and evaluating layers of vulnerability – a way forward' (2019) 19(2) *Developing World Bioethics* https://doi.org/10.1111/dewb.12206

[15] Malgieri and Niklas (n 12).

[16] Peter Blume, 'The Data Subject' (2015) 1(4) *European Data Protection Law Review* https://doi.org/10.21552/EDPL/2015/4/4

[17] Ibid.

Digital citizenship can be defined as the totality of social and technological arrangements that enable individuals to use digital tools to participate in society.[18] Digital citizenship is grounded in digital literacy, that is, the skills needed to navigate the online world and handle digital technologies. It goes beyond individual abilities by encompassing the relationships between individuals and other actors in the digital sphere. The concept of digital citizenship builds on the digital participation of members of society, which presupposes the active interpretation of information flows and the formation of digital identities.[19]

A prerequisite for digital citizenship is thus the digital literacy of citizens. In its absence, those who lack such competencies are excluded not only from social discourse, but also from significant decision-making processes. As a result, social groups that are unable, or only with great difficulty able, to acquire adequate levels of digital literacy qualify as data subjects requiring enhanced protection also from a data protection law perspective. This is because digital literacy affects not only the protection of personal data in the digital environment, but also the prospects for social participation and the exercise of civil rights. If this is accepted, it follows directly that, in the context of society's digital transformation, data protection no longer safeguards only individual but also collective rights. It can moreover be understood as a boundary condition for the formation of digital citizenship, operating as a gatekeeper of individual and collective interactions.



## *2. Data Protection Awareness in the Mirror of Data*

The definition of data subjects, or more precisely the determination of data subject status, is therefore a key issue, as the applicable level of protection is aligned with it. Against this background, it is necessary to examine what empirical data exist on data protection awareness and GDPR knowledge, in particular with regard to individually distinguishable groups of data subjects.

In 2019, at the request of the European Commission, a Special Eurobarometer survey was conducted with the aim of mapping awareness of the GDPR as well as more general attitudes and behaviours regarding data sharing and data protection.[20]

One of the most important findings of this survey, from the perspective of the present study, is that a majority of respondents (67%) had heard of the

[18] Razvan Rughiniş and others, 'From social netizens to data citizens: Variations of GDPR awareness in 28 European countries' (2021) *Computer Law and Security Review*. 42, 1-15. https://doi.org/10.1016/j.clsr.2021.105585

[19] Luci Pangrazio and Julian Sefton-Green, 'Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?'(2021) 10, *Journal of New Approaches in Educational Research* https://doi.org/10.7821/naer.2021.1.616

[20] European Commission. (2019b). Special Eurobarometer 487a: The General Data Protection Regulation. Publications Office of the European Union. Online: https://doi.org/10.2838/579882

GDPR. Of these, 36% had both heard of it and knew what it was, while 31% had heard of it but did not know precisely what it regulated.[21]

On the basis of these results, further interpretative possibilities emerge. Using indicators of GDPR awareness, respondents from the EU-27 and the United Kingdom can be divided into four groups: offline citizens (22%), social netizens (32%), web citizens (17%), and data citizens (29%). Offline citizens show the lowest levels of internet use and GDPR awareness. Web citizens are located around the average values. Data citizens exhibit the highest levels both in terms of digital experience and in terms of GDPR knowledge and usage. The fourth group, social netizens, display a more contradictory profile: their use of social networks is extremely high, their experience with online shopping is below average, and their level of GDPR awareness is likewise below average.[22]

Since 2019, no new comprehensive Eurobarometer survey has been conducted that focuses exclusively and specifically on GDPR awareness. This does not mean, however, that there are no further data on GDPR awareness embedded in other research.

In 2021 and again in 2024, the Eurobarometer carried out comprehensive surveys entitled "Justice, Rights and Values" in the Member States. As a contextual background, it should be noted that, as part of the European Union's 2021--2027 long-term budget, the "Citizens, Equality, Rights and Values" programme and the Justice programme were adopted on 28 April 2021, with a combined budget of 1.8 billion euros. These surveys sought to capture EU citizens' views on the values promoted by these programmes and their knowledge of the various instruments used to promote and protect rights and values.[23] In what follows, the present study analyses the data series generated by the Eurobarometer with regard to the GDPR.



*2.1 Numbers and Tendencies*

The 2019 survey explicitly placed knowledge of the GDPR at the centre of the research. The 2021 and 2024 surveys, although more limited in this regard, nevertheless contain questions that allow for comparison and analysis over time. In the following, the available data series are compared along four main dimensions: (1) the proportion of respondents who had heard of the GDPR in the relevant period; and (2) how awareness is structured according to age; (3) employment status; and (4) financial status. The examination of these three clearly delineated data subject groups provides a suitable empirical foundation for the previously outlined discussion on the concept of the data subject.

[21] Ibid.

[22] Rughiniş and others (n 18).

[23] European Commission. (2021). Special Eurobarometer 514: Justice, Rights and Values. Publications Office of the European Union. https://doi.org/10.2838/3

In 2019, as noted, a majority of respondents (67%) had heard of the GDPR; 36% had heard of it and knew what it was, while 31% had heard of it but did not know exactly what it was. By age group, the highest level of awareness was found among respondents aged 25--54 (75%), followed by respondents younger than this age group (66%), and the lowest level among those older than 54 (58%).[24]

With respect to employment status, managers displayed the highest level of awareness regarding the GDPR (86%), while retired respondents recorded the lowest figure (55%). The Eurobarometer survey also addressed the dimension of financial difficulties. The fewer financial problems respondents faced, the more likely they were to be aware of the Regulation. Among respondents who reported no difficulty in paying their bills, GDPR awareness stood at 71%, while among those for whom paying bills posed serious difficulties, this figure was only 49%.[25]

By the time of the 2021 data collection, a visible improvement could be observed across these indicators.

More than 77% of respondents indicated that they had heard of the GDPR, and 47% reported that they had both heard of and understood the Regulation. Almost one third of respondents in the EU (30%) had heard of the GDPR but did not know exactly what it was, while more than one fifth (21%) stated that they had never heard of it.[26]

In terms of age distribution, 83% of respondents aged 25--39 reported awareness of the GDPR in 2021. This group was followed by respondents aged 40--54 (81%), then by those aged 15--24 (77%), while the least aware group remained respondents aged 55 and over (71%). By employment status, managers again reported the highest level of awareness (90%), followed by other office workers (86%) and the self-employed (84%). Among household employees (63%), retirees (68%), and the unemployed (72%), it was less likely that respondents were aware of the GDPR.



A similar pattern can be observed for financial status. EU citizens who had never experienced difficulties in paying their bills were more likely (80%) to report that they knew the GDPR than those who most often struggled with financial difficulties (69%).[27]

Compared to the positive trends identified in 2021, the 2024 data reveal a certain deterioration in awareness of the GDPR. In summary, more than seventy per cent (72%) of respondents across the EU indicated that they had heard of the GDPR, of whom 40% knew exactly what type of instrument it was. Nearly 32%

[24] Ibid (2019 data).
[25] Ibid.
[26] Ibid (2021 data).
[27] Ibid.

had heard of it but did not have precise knowledge, while 26% stated that they had never heard of the GDPR.[28]

For the individual groups examined, the distribution shows that the 25--39 age group continues to demonstrate the highest level of awareness (79%), followed by those aged 40--54 (76%), those aged 15--24 (71%), and finally those aged 55 and over (65%). The 2024 data also confirm the earlier ranking of employment-based groups. Managers again occupy the first place (85%), followed by office workers and the self-employed (both 80%). Household employees (54%), retirees and the unemployed (both 63%) remain the least aware groups.

In terms of financial status, respondents who never or almost never encountered payment difficulties are more familiar with the GDPR (74%) than those who frequently face financial problems (61%).

Overall, the data series show that, in the EU and the United Kingdom, knowledge of the GDPR increased by an average of ten percentage points between 2019 and 2021. In 2019, there were still 13 countries in which less than 70% of respondents were aware of the GDPR. In contrast, by 2021, 16 countries had more than 80% awareness among respondents. In 2024, however, the average familiarity with the GDPR across the Union decreased by five percentage points compared to 2021. While in 2021 more than 70% of respondents were aware of the GDPR in 24 countries, this was the case in only 19 countries in 2024.[29]



### *2.2 Common Directions and Different Risks*

A decrease in GDPR familiarity can be observed across all examined groups between 2021 and 2024. This trend is particularly worrying in relation to those groups that are most vulnerable, such as young people (15--24 years), retirees, the unemployed, and those facing financial difficulties.

The present study does not provide the framework for an in-depth exploration of the reasons underlying these developments. Nonetheless, it is clear that substantial changes are needed in the field of data protection awareness if the groups most in need of protection are to be adequately safeguarded.

Recital 75 of the GDPR explicitly highlights the processing of personal data of vulnerable natural persons -- in particular children -- in connection with risks of varying likelihood and severity to the rights and freedoms of natural persons. It is important to note, however, that children are mentioned in this context merely by way of example ("in particular"). Taken as a whole, the GDPR accords children a quasi-privileged position, whereas other vulnerable groups are not explicitly identified as such. This leads in practice to controllers applying particularly strict safeguards to the processing of children's data, without necessarily enforcing higher levels of protection in relation to other, similarly vulnerable groups.

[28] Ibid (2024 data).
[29] Ibid.

In this respect, it can be concluded that an absolute understanding of the category of data subjects is not tenable, and that the universal application of the vulnerability concept cannot ensure risk-proportionate protection for natural persons.

### *3. Whose Responsibility Is It to Promote Data Protection Awareness?*

The GDPR identifies two addressees in connection with raising awareness: the data protection officer and the supervisory authority.

Pursuant to Article 39(1)(b) GDPR, the data protection officer is to monitor compliance with the GDPR, with other Union or Member State data protection provisions, and with the controller's or processor's internal policies relating to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. It is important to note that neither the GDPR nor established case law elaborates in detail on the obligation of the data protection officer to raise awareness. This is a serious gap, as the DPO is, in principle, the actor best positioned to contribute effectively to awareness-raising and education within the organisation of the controller or processor.

As regards supervisory authorities, Article 57(1) GDPR provides that, without prejudice to their other tasks under the Regulation, they shall, on their respective territories, promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, with specific attention to activities addressed to children.[30]



Article 57 GDPR thus expressly establishes the promotion of public awareness and knowledge regarding the processing of personal data as a dedicated task of supervisory authorities.

When this obligation is juxtaposed with the demonstrable decrease in data protection knowledge among EU citizens between 2021 and 2024, several questions arise.

The first and most important question is to what extent supervisory authorities in individual Member States can be held responsible for the observed decline in awareness.

Exclusive responsibility clearly cannot be established, as the GDPR merely requires supervisory authorities to "promote" the dissemination of data protection knowledge -- a rather open-ended formulation. Nevertheless, the wording of the GDPR undoubtedly implies a requirement to undertake concrete awareness-raising actions.

It also remains an open question which specific types of action can reasonably be expected of supervisory authorities and which results may be

[30] Regulation (EU) 2016/679, art 57(1).

realistically anticipated from such measures. The present study does not allow for a comprehensive and in-depth analysis of these issues. However, some aspects deserve attention, both from a retrospective and from a forward-looking perspective.

In their analysis of the Polish supervisory authority and the challenges of reflexive regulation in its practice, Pichlak and Gaczol identified five key factors that, in the author's view, merit consideration in assessing the operation and enforcement methodologies of supervisory authorities in all EU Member States: resources, capture, capacities, characteristics of controllers, and inconsistencies of the GDPR.[31]

Among these, the first -- resources -- is of particular relevance. Following the logic of Pichlak and Gaczol's study, resources encompass both material means and human capacity. The issue is illustrated here by reference to three Member State supervisory authorities selected on the basis of GDP per capita: France, which roughly corresponds to the EU average (38,000 euros, EU average 37,600 euros), the Netherlands, which exceeds the Union average (48,900 euros), and Hungary, which is below the average (28,700 euros).[32]

In 2025, the French Data Protection Authority operated with a budget of 28.2 million euros and a staff of 298 persons. Between 2019 and 2024, its staff numbers increased by 62%.[33] In the same year, the Dutch Data Protection Authority disposed of 49 million euros and employed 320 persons, an 89% increase compared to 2021.[34] The Hungarian supervisory authority, the National Authority for Data Protection and Freedom of Information, had a budget of 5.8 million euros in 2025 and 129 employees in the first quarter of 2025, which represents an increase of only 19% between 2021 and 2025.[35]



The absolute size of the budget and the growth in staff numbers cannot, in themselves, serve as the basis for comprehensive conclusions. Nevertheless, it can be stated that, despite the expansion of resources, there is no detectable increase in the effectiveness of national authorities as regards data protection awareness. If resources are not the decisive factor, then, according to Pichlak and Gaczol's interpretation, the combination of the other four elements (with varying weight in each Member State) may be responsible for the unfavourable trends.

[31] Maciej Pichlak and Klaudia Gaczol, 'Simple and advanced reflexivity in GDPR enforcement: empirical evidence from DPA activity' (2023) *International Data Privacy Law* 13(4) https://doi.org/10.1093/idpl/ipad018

[32] European Union, EU countries – Facts and figures https://european-union.europa.eu/principles-countries-history/eu-countries_hu

[33] CNIL, *Status & Composition* (2025) https://www.cnil.fr/en/cnil/status-composition

[34] Autoriteit Persoonsgegevens, *Facts and figures about the AP. Autoriteit Persoonsgegevens* (2025) https://www.autoriteitpersoonsgegevens.nl/en/over-de-autoriteit-persoonsgegevens/feiten-en-cijfers

[35] Nemzeti Adatvédelmi és Információszabadság Hatóság, *2025. I. negyedév személyi juttatások: Bér- és létszámadatok* (2025) https://www.naih.hu/files/3_2_2025_I_negyedev_szemelyi_juttatasok.pdf

As regards capture, generalisations are difficult. The extent to which national supervisory authorities are genuinely independent of political or economic power in their respective countries must be assessed on a case-by-case basis; yet, in many instances, empirical substantiation is hardly possible. The concept of capacities, as used by Pichlak and Gaczol, points to deficits in expertise and cultural competence, which may help explain why certain authorities devote relatively little attention to awareness-raising even when resources would permit more proactive engagement. Finally, regulatory inconsistency and the structure of data controllers in the Member State concerned may also significantly influence the practice of supervisory authorities. In particular, adaptation to specific social and economic realities requires different strategies in different Member States.[36]

Looking back, it should be emphasised once again that the role of data protection officers cannot be overlooked when discussing awareness-raising. While supervisory authorities can exert influence at Member State level, it is the DPO who is best placed to promote the dissemination of knowledge within individual controller organisations. Ideally, this would allow for complementary top-down and bottom-up awareness-raising campaigns.

## III. Artificial Intelligence Literacy

### *1. AI Literacy and Digital Literacy*



The social integration of artificial intelligence (AI) is marked by significant concerns. Research communities, governmental bodies, and non-profit organisations alike have emphasised that AI is far more than a mere technological innovation.[37] Due to its novelty and complexity, it is frequently described as a revolutionary, "next wave" technology.[38] Given its general, horizontal and pioneering nature, AI brings with it not only considerable opportunities, but also risks for individuals and society as a whole, including negative effects that are difficult to foresee and to measure.[39]

Risk perception and, consequently, expectations regarding regulation differ considerably across cultures. A community's perception of threats associated with the unknown, and thus its degree of uncertainty avoidance, has a decisive influence on the chosen regulatory approach to technologies that are perceived as

[36] Pichlak and Gaczol (n 38).
[37] Francesca Foffano, Teresa Scantamburlo and Atia Cortés, 'Investing in AI for social good: an analysis of European national strategies' (2022) 38. *AI and Society* https://doi.org/10.1007/s00146-022-01445-8
[38] Mustafa Suleyman and Michael Bhaskar, *A következő hullám: Mesterséges intelligencia, technológia, hatalom és a 21. század legnagyobb kihívása* (Magnólia 2023).
[39] High-Level Expert Group on AI, *Ethics Guidelines for Trustworthy AI* (European Commission 2019).

risky. Previous studies have shown that societies with a high level of uncertainty avoidance tend to adopt a more critical stance towards new technologies.[40]
In addition to differences in risk perception, there are also significant divergences between countries regarding the normative orientation of AI regulation.[41]
With regard to emerging technologies, the pace of technological development inevitably outstrips the speed of regulatory responses. In the case of AI, widespread public uncertainty is more pronounced than ever, and governmental responses alone are no longer sufficient to address questions relating to the benefits, risks and future potential of this technology.[42] This, in itself, is likely to increase uncertainty and shift risk perception in a more negative direction.

Research nonetheless suggests that there are global patterns in AI regulation and in public perception of AI. These include shared assumptions about the economic consequences and impacts of AI, i.e. the recognition of the challenges and opportunities associated with AI and their incorporation into public policy thinking in many countries. At the same time, it is noteworthy that the "European" conception of restrictions on individual AI systems has not found broad support in global public opinion.[43]

One of the most important determinants of the risks and impact of artificial intelligence is the way in which the technology is used. Usage, in turn, directly depends on users' knowledge and understanding and thus on their AI literacy.



At first glance, the concepts of data protection awareness and AI literacy appear to differ. However, both are grounded in similar regulatory logics and expectations. Unlike the GDPR, which relies on the notion of "awareness", the AIA relies on the concept of "literacy".

There is, and is unlikely to be, a uniform, globally accepted general definition of AI literacy. It is therefore useful to begin by delineating the main elements of literacy as they appear in the AIA, before turning to concepts developed in scholarly literature.
Article 3(56) AIA defines "AI literacy" as:[44] "skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their

[40] Bartosz Wilczek, Sina Thäsler-Kordonouri and Maximilian Eder, Government regulation or industry self-regulation of AI? Investigating the relationships between uncertainty avoidance, people's AI risk perceptions, and their regulatory preferences in Europe' (2025) 40(5) *AI & Society* https://doi.org/10.1007/s00146-024-02138-0

[41] Soenke Ehret, 'Public preferences for governing AI technology: comparative evidence' (2022) *Journal of European Public Policy* https://doi.org/10.1080/13501763.2022.2094988

[42] Wendell Wallach and Gary Marchant, 'Toward the Agile and Comprehensive International Governance of AI and Robotics' *Proceedings of the IEEE*, 107(3), 505–508 https://doi.org/10.1109/JPROC.2019.2899422

[43] Ehret (n 48).

[44] Regulation (EU) 2024/1689, art 3(56).

respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause."

Recital 20 supports and refines this definition. It states that the aim of AI literacy is to provide "providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems", to enable them to appropriately interpret the output of AI systems, and to ensure that they are aware of the impact of such systems' decisions on them.[45]

In its "Discussion Paper on Draft Recommendation on AI literacy" published in February 2025, the Council of Europe identified three main dimensions of AI literacy: technological, practical and human. The technological dimension concerns understanding how AI systems work and how they can be further developed. The practical dimension focuses on the ability to use AI effectively. The human dimension relates to the impact of AI on people, human rights, democracy and the rule of law.[46]

As this already indicates, the AIA does not provide an exhaustive definition of AI literacy, but only outlines its main aspects. This is confirmed by Recital 20, which specifies that the required level of understanding may vary depending on the context.[47]

In general terms, AI literacy can be described as the set of competencies that enable individuals to interact effectively with AI technologies. This includes an understanding of basic AI concepts, the ability to critically evaluate AI systems and their outputs, and the ethical use of AI tools in different contexts.[48]



The challenge of defining AI literacy is well known in the scholarly literature, and numerous concepts have been proposed in recent years. Kandlhofer and co-authors, for instance, define AI literacy as the capacity to understand the basic techniques and concepts underlying AI, particularly as they are applied in specific products and services.[49] Ng and co-authors conceptualise AI literacy as a complex body of knowledge that encompasses understanding basic AI functions and applications, the ability to use and apply AI, to evaluate and create AI systems,

[45] Ibid, Recital 20

[46] Council of Europe, *Discussion Paper on Draft Recommendation on AI Literacy* (2025) https://www.coe.int

[47] Regulation (EU) 2024/1689, Recital 20

[48] Yueqiao Jin , Roberto Martinez-Maldonado, Dragan Gašević, Lixiang Yan, 'GLAT: The generative AI literacy assessment test' (2025) *Computers and Education: Artificial Intelligence* https://doi.org/10.1016/j.caeai.2025.100436

[49] Martin Kandlhofer, Gerald Steinbauer, Sabine Hirschmugl-Gaisch and Petra Huber, 'Artificial intelligence and computer science in education: From kindergarten to university' (2016) in *IEEE Frontiers in Education Conference (FIE)* https://doi.org/10.1109/FIE.2016.7757570

and to understand AI ethics and human-centric considerations.[50] Other approaches emphasise technical understanding, practical application, critical ability, efficiency, and the quality of AI-generated outputs.[51]

The definition of AI literacy also depends significantly on the target group of the assessment. Here, it is useful to distinguish between experts and non-experts, i.e. laypersons. For the latter, Laupichler and co-authors propose an assessment framework comprising three components: technical understanding of AI, critical evaluation, and practical application.[52]

All of the above concepts share a similar conceptual lineage with digital literacy. In contemporary knowledge-based societies, digital literacy denotes the basic digital competencies that all citizens must possess in order to enjoy equal opportunities in the labour market.[53]

The origins of digital literacy can be traced back to the 1960s. However, its definition has evolved continuously alongside technological developments and the changing environments to which it refers.[54] Initially, digital literacy was associated primarily with the visual processing of information, a notion captured in John Debes' concept of "visual literacy".[55]

With technological advancement, the semantic content of digital literacy has changed, and there is still no widely accepted, fully standardised definition. Different authors define digital literacy in different ways, as the evolution of the technological environment and the pace of innovation significantly influence how people use digital tools. At the same time, there is broad agreement that digital literacy is a multidimensional construct encompassing technical and cognitive skills, metacognitive processes, civic engagement, and ethical awareness.[56]



[50] Davy Tsz Kit Ng, Jac Ka Lok Leung, Samuel Kai Wah Chu and Maggie Shen Qiao, Conceptualizing AI literacy: An exploratory review' (2021) *Computers and Education: Artificial Intelligence* https://doi.org/10.1016/j.caeai.2021.100041

[51] Senad Bećirović , Edda Polz1 and Isabella Tinkel, 'Exploring students' AI literacy and its effects on their AI output quality, self-efficacy, and academic performance ' (2025) 12(29) *Smart Learning Environments* https://doi.org/10.1186/s40561-025-00384-3

[52] Matthias Carl Laupichler, Alexandra Aster, Nicolas Haverkamp and Tobias Raupach, Development of the "Scale for the assessment of non-experts' AI literacy" – An exploratory factor analysis' (2023) *Computers in Human Behavior Reports* https://doi.org/10.1016/j.chbr.2023.100338

[53] David Bawden, 'The distractions of documentation' (2008) *Journal of Documentation* https://doi.org/10.1108/jd.2008.27864faa.001

[54] Nikitas Kastis and Roberto Carneiro,' Digital Literacy—The Evolution of the 21st Century Literacies' (2009) https://www.openeducationeuropa.eu/en/paper/digital-literacy-%E2%80%93-evolution-21st-century-literacies

[55] Colin Lankshear and Michele Knobel, 'Digital Literacies: Concepts, Policies and Practices' (2008) *Peter Lang Publishing*

[56] Pritika Reddy, Bibhya Sharma and Kaylash Chaudhary , 'Digital Literacy: A Review of Literature' (2020) 11(2) *International Journal of Technoethics (IJT)* https://doi.org/10.4018/IJT.20200701.oa1

Balázs Hohmann considers digital literacy the foundation of all meaningful platform regulation, as it enables individuals to find, understand and critically evaluate the services they use.[57]

The measurement of AI literacy raises additional methodological challenges. While knowledge of the GDPR can be probed through relatively clear and measurable questions, the assessment of AI literacy requires more differentiated instruments.

Existing measurement tools largely rely on self-assessment, while performance-based instruments are used much less frequently. This raises questions about the reliability of survey data. Although performance-based tests exist for general AI literacy -- for example, the Hornberger test -- there is, as yet, no suitable methodology for assessing knowledge of generative AI (GenAI). Without performance-based instruments, self-reporting biases cannot be adequately controlled, particularly in relation to new technologies such as AI and GenAI tools.[58]

## IV. Conclusion

The working hypothesis of this research was that the foundations of data protection awareness and AI literacy can be aligned and that experiences gained following the entry into force of the GDPR could usefully inform the implementation of the AIA. Comparing the concepts and legal content of data protection awareness and AI literacy is far from straightforward. Nevertheless, the assertion that both are prerequisites for digital literacy -- that is, for the capacity of users to know and understand the nature of their use of digital tools -- appears well founded.



The GDPR does not define data protection awareness. However, on the basis of the literature and the tasks assigned to data protection officers and supervisory authorities, it can be interpreted as a special form of legal awareness that extends to the rights deriving from the GDPR, to their content, and, where appropriate, to the obligations flowing from the Regulation.

AI literacy, particularly as conceptualised in the AIA, has a more technology-focused semantic content, emphasising concrete use of AI systems, their results and their evaluation. The two normative concepts also relate to partially different personal scopes. As regards data subjects, the GDPR places the obligation to promote data protection awareness on data protection officers and supervisory authorities. By contrast, the AIA assigns responsibility for ensuring AI literacy to providers and deployers of AI systems. In this context, neither fundamental rights authorities under Article 77 AIA nor market surveillance authorities have a direct

[57] Balázs Hohmann, 'The Interplay Between User Awareness And Transparency Requirements In The Context Of European Platform Regulation' (2025) *Journal Of Humanities and Social Science* (IOSR-JHSS) 30 (8) https://doi.org/10.9790/0837-3008052433

[58] Jin and others (n 55).

role. Only in relation to the European Artificial Intelligence Board (hereinafter: Board) does the legislator refer to awareness-raising, providing in Article 66(f) that the Board may support the Commission's "public awareness-raising activities on AI literacy and the use of AI systems".

Ultimately, both normative concepts aim to enhance the protection, awareness and knowledge of "end users". A further commonality is that both build on digital literacy and can be regarded as its specific manifestations.

Unlike the GDPR, however, the AIA does not require public authorities to develop literacy. It essentially treats literacy as an obligation incumbent solely upon providers and deployers. Consequently, it can be concluded that, while the AIA defines the concept of literacy, it does not render it enforceable through the instruments of public authorities.

In light of the empirical findings presented in this study, it is doubtful that this legislative approach will lead to satisfactory outcomes. A decrease in data protection awareness -- particularly among vulnerable groups -- can be demonstrated despite the fact that, over the same period, data protection authorities performed their tasks with increasing budgets and staff numbers. If this is recognised as a broader trend, even in a regulatory environment in which the allocation of responsibility is more clearly defined and is shared between two main addressee groups (supervisory authorities and controllers through data protection officers), it is not immediately apparent why one should expect better results in a regime in which only one of these groups has been designated (providers and deployers).



Based on the research presented, the social environment from which the persons "protected" by these normative concepts originate cannot be ignored. In the context of the GDPR, Eurobarometer data show that the social and sociocultural background of data subjects is relevant. When the same question is posed in relation to the AIA, however, attention must be paid not only to individuals' prior education, but also to the broader attitudes prevailing in the social environments in which they live.

Continuing this line of thought, it must also be noted that the concept of AI literacy as employed in the AIA is overly restrictive, as it fully excludes those who do not use or deploy a given AI system, yet are nonetheless affected by it. This gap cannot be filled by reference to the seven principles laid down in the AIA either. Against this background, it is particularly problematic that the AIA does not establish a uniform supervisory authority system comparable to that of the GDPR, thereby preventing the emergence of corrective mechanisms that could potentially arise from authority involvement.

In light of the experiences and data accumulated under the GDPR and considering the horizontal risk exposure of AI systems, it remains an open question which control mechanisms will ultimately be applicable in practice.

## STATEMENTS

### Disclosure statement
No potential conflict of interest was reported by the author.

### Funding
The author received no financial support for the research, authorship, or publication of this article.

### Data deposition and availability
There is no data set associated with the study. No data deposition was required for this study.

### Use of Artificial Intelligence
The author acknowledges the use of Perplexity AI for translation assistance. The author has reviewed and edited the AI-generated translation to ensure accuracy, clarity and appropriate legal terminology, and assumes full responsibility for the final content of this article.

### Author contributions (CRediT)
Conceptualization; Methodology; Investigation; Formal analysis; Resources; Data curation; Writing – Original Draft; Writing – Review & Editing.

# A KRIMINALISZTIKAI ROBOTIKA AKTUALITÁSAI ÉS AZ INTEGRÁLT BIZTONSÁGI RENDSZEREK

*Dr. Csete Róbert*
*Végzett joghallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Kar*
*A szerző elérhetősége: cseterobert2@gmail.com*
*ORCID: 0009-0008-4709-1225*

**DOI: 10.47272/KIKPhD.2025.3.2**

## ABSZTRAKT

Az elmúlt két évtized technológiai fejlődése — különösen a robotika és a mesterséges intelligencia (MI) terén — új lehetőségeket teremt a kriminalisztika számára. Autonóm és távirányított technológiai megoldások — legyenek azok szárazföldi, légi vagy más speciális rendszerek — immár valós kiegészítő eszközei a kriminalisztika gyakorlatának.

A tanulmányba foglalt megállapítások alapján a vizsgált technológiák képesek lehetnek a jelenleginél is hatékonyabban szolgálni a rendfenntartókat, ha integrált rendszerként működnek: szenzorfúzióval, valós idejű adatkezeléssel és ember-gép együttműködéssel. Ebben a tanulmányban igyekszem bemutatni, miként vázolható fel egy ilyen integrált kriminalisztikai robotikai rendszer, és rávilágítani arra, hogy a működéséhez szükséges technológiai megoldások milyen formában állnak rendelkezésünkre.



## KULCSSZAVAK

Kriminalisztikai robotika; autonóm rendszerek; drónok; robotkutyák; integrált biztonsági rendszerek.

## KÉZIRATTÖRTÉNET

BENYÚJTVA 2025.11.16. | FELÜLVIZSGÁLVA 2025.11.30. | ELFOGADVA 2025.12.03.

## I. Bevezetés – Kriminalisztika és az autonóm rendszerek

Ahhoz, hogy a megfelelő alapokra támaszkodva vizsgáljuk meg a témát elengedhetetlen, hogy szemlézzük a legalapvetőbb vonatkozó fogalmakat. Viski László a következőképpen határozta meg a kriminalisztikát:

*„A kriminalisztika a bűncselekmények nyomozásának, felderítésének tudománya. Célja, hogy a tételes jog által meghatározott keretekben olyan módszereket és eljárásokat dolgozzon ki, amelynek a segítségével a készülő bűncselekmények* ***leleplezhetők, megakadályozhatók****, a már elkövetett bűncselekmények* ***felderíthetők****, elkövetőjük megállapítható és felelősségre vonható."*[1]

E fogalmat alapul véve megállapíthatjuk, hogy a tanulmányban bemutatandó technológiai megoldásoknak és integrált rendszereknek legalább az elméleti síkon alkalmasnak kell lenniük arra, hogy a még el nem követett bűncselekményeket megelőzzék, a már elkövetetteket pedig eredményesen felderítsék. A megfogalmazás, miszerint ezek a rendszerek előzik meg, derítik fel a bűncselekményeket, azonban igencsak félrevezető. Ennek oka abban rejlik, hogy az autonóm rendszereket az alábbiak szerint két csoportra osztjuk:

*„Az a szabadság, amellyel egy rendszer rendelkezik a beprogramozott célok megvalósításához. Az autonóm rendszerek lehetnek* ***fél-autonómok****, amelyek működésébe emberi tényező kapcsolódik („ember a folyamatban"), illetve* ***teljesen autonómok****, amelyek a rájuk bízott feladatokat emberi beavatkozás nélkül képesek végrehajtani."*[2]

Ahogyan azt a tanulmány vonatkozó részeiben is látjuk majd, a jelenleg elérhető technológiai fejlettségi szint nem teszi lehetővé, hogy a felhasznált platformok érdemben és megbízható módon tudhassák sajátjuknak a teljes autonómiát, emellett a fejlesztésből - a mesterséges intelligencia alapú technológiák szabályozását meghatározó jogalkotói törekvések sarkalatosnak tűnő pontja szerint - sem hagyható ki az „ember a folyamatban" tényező. A kizárólag kiegészítő funkciót lehetővé tevő környezet mellett azonban nem hagyhatjuk figyelmen kívül azt a tényt, hogy a robotika párhuzamos fejlődése kibővíti a lehetőségeket, hiszen *„[...] robotok fejlesztésére összpontosít – olyan gépekre, amelyek képesek összetett műveletsorok végrehajtására, és távolról irányíthatók vagy autonóm módon működhetnek. A robotika magában foglalja a robotok tervezését, építését, működtetését és alkalmazását, valamint az ezek irányításához, szenzoros visszacsatolásához és információfeldolgozásához – például mesterséges intelligenciához – szükséges számítógépes rendszereket."*[3]



[1] Csaba Fenyvesi, Csongor Herke and Flórián Tremmel, *Kriminalisztika (*Ludovika Egyetemi Kiadó 2022) 27.

[2] INTERPOL, UNICRI: 'Artificial Intelligence and robotics for law enforcement' https://unicri.org/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf accessed 2026.01.04.

[3] INTERPOL, UNICRI: 'Artificial Intelligence and robotics for law enforcement' https://unicri.org/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf accessed 2026.01.04.

A fentiek alapján nagy bizonyossággal kijelenthető, hogy míg a XIX-XX. században a természettudományok vívmányai hoztak el gyökeres változásokat a kriminalisztika világába, úgy a XXI. században hasonló hatást érhet el a robotika és a mesterséges intelligencia fejlődése.

## II. A felhasználható platformok

Ebben a fejezetben veszem sorra azokat a platformokat és a rájuk épülő technológiai megoldásokat, amiket a téma szempontjából leginkább érdemes megvizsgálni. A platformokat három csoportra: pilóta nélküli légijármű-rendszerekre, robotkutyákra és biztonsági robotokra osztottam. Mindhárom csoportnál arra törekszem, hogy a lehető legnaprakészebb adatokkal és az elmúlt egy-két év gyakorlatából hozott példákkal támasszam alá megállapításaimat.

### 1. Pilóta nélküli légijármű-rendszerek

A hatályos magyar jogszabályok értelmében pilóta nélküli légijárműnek (a továbbiakban: drón) minősül:

*„bármely olyan légi jármű, amely a fedélzetén tartózkodó pilóta nélkül üzemel vagy amelyet ilyen üzemmódra terveztek, és amely önálló vagy távirányítással történő üzemelésre képes."*[4]

A fenti kategóriába tartozó gépek rohamos fejlődésen estek át köszönhetően egyrészt a drónhadviselés korszakának[5], másrészt az egyre gyakoribb kriminalisztikai alkalmazásnak.



Az Orosz-Ukrán Háborúban megörökített számtalan dróntámadás[6], a húszi lázadók Vörös-tengeren folytatott zaklató műveletei[7], a mianmari junta csapásai[8] vagy éppen a kolumbiai kartellek akciói[9] mind azt bizonyítják, hogy a drónok használata polgári és kereskedelmi használaton túli világot is meghódítani igyekszik, vagy már talán meg is hódította azt. A sikeres támadóműveleteket azonban megelőzi egy másik, a kriminalisztika szempontjából sokkal lényegesebb tevékenység: a felderítés. A drónok alkalmazása lehetővé teszi a valós idejű megfigyelést a lehető legtágabb értelemben véve. Azt, hogy ez pontosan mit is jelent a gyakorlatban, egyre gyakrabban láthatjuk a világ rendőrségei által a közvélemény számára hozzáférhetővé tett felvételeken.

[4] 1995. évi XCVII. törvény a légiközlekedésről, 71. § 35. pont

[5] 'HadERŐ: sikeresen vizsgáztak katonáink az Adaptive Hussars 2025 gyakorlaton' https://honvedelem.hu/magazin/hadero-sikeresen-vizsgaztak-katonaink-az-adaptive-hussars-2025-gyakorlaton.html accessed 2026.01.04.

[6] Gábor Farkas, Gábor Fazekas and András Németh, 'FPV-drónok detektálásának alternatív megoldása konvolúciós neurális hálózattal' (2025) 2 *Haditechnika* 2 https://doi.org/10.23713/HT.59.2.01

[7] 'EUNAVFOR Operation ASPIDES: EUNAVFOR ASPIDES: One month since the launch of the Operation' https://www.eeas.europa.eu/eunavfor-aspides/eunavfor-aspides-one-month-launch-operation_en?utm_ accessed 2026.01.04.

[8] Thomas H. Andrews, 'Report of the Special Rapporteur on the situation of human rights in Myanmar' https://www.ohchr.org/sites/default/files/documents/countries/myanmar/a-80-490-auv-en.pdf?utm_ accessed 2026.01.04.

[9] Andrés Julián, https://x.com/AndresJRendonC/status/1958578176914800916

2025. március 1. napján a Chicói Rendőrség (Amerikai Egyesült Államok, Kalifornia) egy lövöldözés elkövetőjét kísérelte meg elfogni, amikor az elkövető, Michael Oxley egy közeli épületkomplexumba menekült. A rendőrök az érintett épületeket körbezárták, majd egy drónt küldtek be annak érdekében, hogy felderítést végezzenek. A drón kamerájának felvételein látszik, hogy Oxley egy maroklőfegyverrel és medveriasztó sprével a kezében várja a rendőröket. Az észlelést követően a drónpilóta a drónra szerelt zavaró eszközök bevetésével a komplexumhoz tartozó parkolóházba üldözi Oxleyt. A parkolóház legfelső emeletére, egy nyílt és tágas területre szorult Oxleyt végül egy kétórás eredménytelen tárgyalás és az általa leadott lövések után a rendőrök agyonlőtték. A drónnak köszönhetően elhárult annak a veszélye, hogy a rendőröknek egy kiemelten kockázatos környezetben, egy hosszú zárt folyosón kelljen szembeszállniuk az elkövetővel.[10]

2025. február 13. napján Darányban drón segítségével[11] sikerült felderíteni egy éppen bűncselekmények elkövetésére készülő apa-fia párost. A Magyar Rendőrség közleménye szerint:[12] *„[…] a hatóság tudomására jutott, hogy egy gyanúsan viselkedő páros, feltehetőleg betörők járják Darány utcáit. A rendőrök haladéktalanul megkezdték az adatgyűjtést és a tanúkutatást, valamint drónt vetettek be. Kisvártatva a drónkezelő észrevette, amint egy ház udvarából tart kifelé az egyik feltételezett gyanúsított, társa eközben a kocsiban várakozott. A férfi éppen elsétált volna a helyszínről, amikor a rendőrök elfogták, míg tettestársa az autóval próbált meg elmenekülni, azonban őt is hamarosan utolérték és elfogták. Mindkettőjüket előállították a Barcsi Rendőrkapitányságra […]"*



2025. január 1. napján a Szingapúri Rendőrség (SPF), mely a világ egyik legfejlettebb eszközöket alkalmazó rendőrségének számít, drónokat vetett be újévi ünnepségen:[13]

*„Az SPF drónokat és mesterséges intelligenciát (MI) is alkalmazott a kiemelt rendezvények biztosításának támogatására. A Marina Bay Singapore Countdown esemény során az SPF együttműködött a Home Team Science & Technology Agency-vel (HTX), és egy MI-alapú videoanalitikai eszköz, a Q-Crowd Counter segítségével elemezte a drónok valós idejű felvételeit. Az eszköz lehetővé tette az SPF számára a tömeglétszám pontosabb helyzetértékelését, valamint az esemény alatti szükség szerinti reagálást."*

Ugyan a fenti esetek csupán egy apró szeletét jelentik azoknak az alkalmaknak, amikor a bűnüldöző szervek drónokat vetettek be 2025-ben, három dolog mégis megállapítható. Elsőként az, hogy a drónok kriminalisztikai célú felhasználása egyáltalán nem a tudományos-fantasztikus jövőkép egyik ábrándjai,

[10] Chico Police Department, https://www.facebook.com/reel/1349442639905635 accessed 2026.01.06.
[11] Somogy Vármegyei Rendőrség, https://www.facebook.com/61556109240200/videos/9063986150364136/ accessed 2026.01.04.
[12] Magyar Rendőrség, 'Drón segítségével érték tetten a betörőket' https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/dron-segitsegevel-ertek-tetten-a-betoroket accessed 2026.01.04.
[13] Singapore Police Force Annual 2024, 'A future-ready Singapore Police Force: Cyber and beyond' 12.

hanem nagyon is a jelen tényezői. Másrészt az, hogy a drónok igenis alkalmasak a bűncselekmények felderítésére, megakadályozására és leleplezésére. Elősegítik az elkövetők azonosítását, a történeti tényállások feltárását és rekonstrukcióját. Változatos szerepkörökben állnak helyt és megfelelő platformként szolgálnak és szolgálhatnak MI-alapú technológiai megoldások számára is. E két megállapításból következik a harmadik, miszerint a drónok bizonyított hasznossága azt eredményezi, hogy a világ rendőrségei és egyéb hatóságai az eszköztáruk, gondolkodásmódjuk, doktrínájuk részévé teszik a drónokat. Egyebek mellett ez azt is eredményezi, hogy a kifejezetten kriminalisztikai szempontokat figyelembe vevő technológiai fejlesztések száma növekszik.

## 2. Robotkutyák

A robotkutyákkal kapcsolatban szinte kivétel nélkül ugyanezeket a megfigyeléseket és megállapításokat tehetjük. Ezek a jellemzően négylábú robotok különféle érzékelőkkel és mechanikus modulokkal felszerelhetők, illetve kiegészíthetők. Alapvetően vezetéknélküli kapcsolaton keresztül, egy képzett kezelő irányítja őket, ám egyes példányok alkalmasak előre meghatározott útvonalon autonóm módon közlekedni, felderítést vagy járőrözést végezni. Az általam fellelt és vizsgált esetek többségében a Hyundai Motor Group portfóliójához tartozó Boston Dynamics nevű egyesült államokbeli vállalkozás „Spot" termékmegnevezést viselő robotkutyája került bevetésre kriminalisztikai céllal. Az Európai Unió 27 tagállamából csupán 6-nál találtam rendvédelmi alkalmazásról szóló megbízható forrásokat.



Magyarországon a Terrorelhárítási Központ (a továbbiakban: TEK) állította szolgálatba Spotot[14]. A műszaki felderítő eszköztár részét képező robotról Pusztai Béla alezredes így nyilatkozott:

*„A robotképességünk már hosszú évek óta megvan, […] Ezek a ma elérhető csúcstechnológiánál lassabbak voltak, mivel minden mozdulatukat az operátornak kellett vezérelnie, előre megtervezve a szükséges mozgásformát. A Spot robotkutya […] azonban integrált mesterséges intelligenciával dolgozik, így képes önállóan korrigálni a talaj egyenetlenségeit, lépcsőt mászni vagy épp egy egyszerű parancsot követően ajtót nyitni."*

Németországban, Baden-Württemberg tartományban a helyi rendőrség különleges egysége alkalmazza Spotot[15]. Thomas Strobl tartományi belügyminiszter az átadáskor kiemelte, hogy:

[14] Magyar Rendőrség, 'Spot, a TEK robotkutyája' https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/spot-a-tek-robotkutyaja accessed 2026.01.04.

[15] Polizei Baden-Württemberg, *Übergabe des Roboter-Hundes „Spot" an die Spezialeinsatzkräfte der Polizei Baden-Württemberg Innenminister Thomas Strobl. „Hightech-Helfer wird unsere Einsatzkräfte zukünftig tatkräftig unterstützen"* https://www.polizei-bw.de/uebergabe-des-roboter-hundes-spot-an-die-spezialeinsatzkraefte-der-polizei-baden-wuerttemberg-innenminister-thomas-strobl-hightech-helfer-wird-unsere-einsatzkraefte-zukuen/ accessed 2026.01.04.

*„[…] Gyorsabbak, és a helyszínen kevesebb nyomot zavar-nak meg, mint a hagyományos, kerekeken vagy lánctalpakon közlekedő robotok, amilyeneket például már a tartományi bűnügyi hivatalunk is használ. […]"*

Az olasz Csendőrség (Arma dei Carabinieri) „Saetta" néven állította csatasorba Spotot[16], elsődlegesen azzal a szándékkal, hogy radioaktív, vegyi és robbanóanyagok jelenlétét észlelje és jelentse, valamint eszközként részt vegyen azok biztonságos ártalmatlanításában.

A fenti képességek által nyújtott lehetőségeket kiaknázva Hollandiában kábítószer-laboratóriumok átfésülésére[17], a spanyolországi Malagában a járőrözést szem előtt tartva kísérletezett a rendőrség a helyi egyetem robotkutyájával[18], a Finn Nemzeti Rendőrség pedig egy kínai vállalkozás arcfelismerő rendszerekkel rendelkező robotkutyáját használja járőrözésre és megfigyelésre.[19]

Az Egyesült Államokban és a Kínai Népköztársaságban (a továbbiakban: Kína) azonban korántsem olyan nehéz példákat találni a robotkutyák kriminalisztikai alkalmazására, mint az Európai Unióban. Tekintettel arra, hogy a vonatkozó termékeket ehhez a két országhoz kötött vállalkozások gyártják ebben nincs semmi meglepő.

A Bloomberg 2025-ös értesülései szerint csak Spotot több mint hatvan rendfenntartó szerv alkalmazza az Egyesült Államokban és Kanadában.[20] A sajtóértesülések mellett pedig hozzáférhető számtalan hivatalos és hiteles forrás arról, hol és miképpen vetik be Spotot és más gyártók robotkutyáit az amerikai hatóságok.[21] A hagyományos tűzszerész és taktikai feladatokon túl a járőrözés és azon keresztül a felderítés, a bűncselekmények megelőzése és kriminalisztikai szempontból releváns adatok összegyűjtése is osztályrészükül szolgál.

Kínában a nagyvárosok utcáin és a turisztikai szempontból kiemelkedően fontos területeken végzett járőrtevékenység kap nagyobb hangsúlyt. Legalábbis erre



[16] typo, I Carabinieri arruolano Saetta, il primo cane robot basato su Spot di Boston Dynamics https://www.typomedia.co/tecnologia/carabinieri-arruolano-saetta-primo-cane-robot-spot-boston-dynamics accessed 2026.01.04.

[17] Reuters, 'Dutch police introduce 'Robodog' for drugs lab investigations' https://www.youtube.com/watch?v=FO_36bxKaIE accessed 2026.01.04.

[18] Universidad de Málaga, 'MÁLAGA, EPICENTRO DE LA INNOVACIÓN EN SEGURIDAD AL PROBAR LA POLICÍA LOCAL UN PERRO ROBOT DISEÑADO POR LA UMA' https://www.malaga.eu/visorcontenido/ANUDocumentDisplayer/172841/NOTAINFORMATIVA.pdf accessed 2026.01.04.

[19] UNOGAI, 'Robodogs on Patrol: Kuusoma, Finland's AI Policing Success Story' https://unogai.org/ai-technology/robodogs-on-patrol-kuusoma-finlands-ai-policing-success-story/ accessed 2026.01.04.

[20] Bloomberg Technology: HU
'A Robot Dog Is Becoming Standard in Policing — and Raising Ethical Alarms' https://www.youtube.com/watch?v=RRUgVKVGznQ&list=PLuE7CXW07-ZTENUinZfX5JI3CfuS6yZBH&index=72 2026.01.04.

[21] Csete Róbert, 'Mesterséges Intelligencia a kriminalisztikában – Alkalmazások és tapasztalatok. Szakdolgozat' (Pécsi Tudományegyetem 2024)13-14.

lehet következtetni az állami hírügynökségek cikkeiből[22] és számos közösségimédia-bejegyzésből. A szóban forgó kép- és videófelvételeken jellemzően a menetelő rendőrök oldalán vagy éppen őrszolgálatuk teljesítése közben láthatók a robotkutyák.[23] Többször középpontba kerül emellett, hogy a robotkutyák hálóvetővel[24], hangszórókkal felszerelhetők, valamint, hogy érzékelőiknek köszönhetően alkalmasak gyanús testmozgások és tárgyak felismerésére, bejelentésére.

### 3. Biztonsági robotok

A biztonsági robotokat egyrészt az különbözteti meg a robotkutyáktól, hogy jellemzően épületek, nagyobb létesítmények védelmére használják őket, ezen belül is főként beltéri járőrözésre alkalmasak. A durva terepen is helytálló és mozgékonyságot kölcsönző mechanikus lábak helyett kerekeken közlekednek. Külsőjük rendszerint „dobozszerű". Működési elvük ettől függetlenül nem sokban tér el a robotkutyáknál megfigyelttől. Adott egy mobil platform, amit különféle kamerákkal, érzékelőkkel szerelhetnek fel, ezzel elősegítve a kiterjedt objektumvédelmet.

Az Egyesült Államokban több vállalkozás is foglalkozik biztonsági robotok fejlesztésével és forgalmazásával. A kutatásom során a Knightscope K5-ös robotjával kapcsolatban leltem fel a legtöbb hitelesnek minősíthető adatot és alkalmazási példát, így ezen a roboton keresztül mutatom be az ország biztonsági robotokkal kapcsolatos legfontosabb eredményeit.



A K5-ös körülbelül 165 cm magas és 190 kg súlyú. Kerekeken közlekedik, legfeljebb 4,8 km/h sebességgel. A gyártó szerint képes a 24-órás autonóm megfigyelésre és járőrözésre, emellett MI-alapú rendszereinek köszönhetően potenciális veszélyt jelentő mintákat ismer fel az emberek magatartásában és környezetében. A Knightscope és a robotot alkalmazó állami és magánjellegű szereplők adatai szerint azokon a helyeken, ahol bevetették a K5-öst, egyértelmű javulás történt a bűnügyi statisztikákban.[25] [26]

Huntington Park City rendőrfőnöke, Cosme Lozano így számolt be tapasztalatairól a város vezetésének:

*„Nos, a valóság az, hogy egy rendőrjárőr nem képes arra, amire a modern technológia ezen a roboton keresztül képes. A robot egyik legjelentősebb tulajdonsága, hogy a hét minden*

[22] Global Times, 'Robot dog begins field patrol in Hangzhou, advancing AI powered urban governance' https://www.globaltimes.cn/page/202510/1345800.shtml?utm_ accessed 2026.01.04.

[23] China Xinhua News, 'Robotic dogs assist police with patrols in SW China' https://www.facebook.com/XinhuaNewsAgency/videos/1039806871345717/ accessed 2026.01.04.

[24] CGTN, 'Sichuan police deploy robot officers to assist in traffic control' https://www.youtube.com/watch?v=uCFb5f4KAEw accessed 2026.01.04.

[25] Knightscope, 'It's All About the Results!' https://knightscope.com/hubfs/664f7aee27918ece47e8f024_24Q2%20Crime%20Stats.pdf?hsLang=en accessed 2026.01.04.

[26] Knightscope, 'Case Studies' https://knightscope.com/crime accessed 2026.01.04.

*napján, a nap mind a huszonnégy órájában magas felbontású felvételeket készít a környezetében történő eseményekről. Rendelkezik egy vészhívó gombbal is, amin keresztül a park látogatói szükség esetén felvehetik a kapcsolatot a segélyhívóközpont munkatársaival. […]"*

Lozano rendőrfőnök felhívta a figyelmet a rendszámtábla-leolvasó rendszerre is, ami lehetővé teszi, hogy egy nyomozás keretein belül ellenőrizzék, járt-e az adott bűncselekményhez köthető gépjármű a robot által ellenőrzött területen. Ez a funkció Kansas Cityben már elkövetők sikeres elfogáshoz is vezetett.[27]

A versenytárs, Kína szintén több fejlesztést tud felmutatni. A robotkutyákhoz hasonlóan elsődlegesen a rendőrökkel való közös járőrözésre szánják az eddig tesztelt vagy szolgálatba állított példányokat. Némileg szokatlan, gömbformájú robot[28] és – inkább helyhez kötött, nem mobil - humanoid robotokról[29] van szó, ám ezek eredményes felhasználásáról megbízható információkat azon túl, hogy kameráikkal adatokat rögzítenek, nem találtam.

Mivel a humanoid biztonsági robotok alkalmazása a kutatás eredményei alapján egyelőre nem gyakori jelenség és véleményem szerint nem sorolhatók a biztonsági robotokkal egy kategóriába, bővebben nem tárgyalom a témát. Fontosnak tartom azonban megemlíteni a Boston Dynamics Atlas nevű robotját, mely figyelemreméltó előrehaladást ért el a közelmúltban.[30]

Ugyan az Egyesült Államok és Kína az utóbbi években – részben a kialakult versengésnek köszönhetően - jelentős sikereket ért el a robotika és az MI-fejlesztések területén, álláspontom szerint Japánban a többi vizsgált országhoz képest már korábban is nagyobb hangsúlyt kaptak a biztonsági robotokhoz kapcsolódó technológiai megoldások.[31]



2025-ben a SECOM cocobo nevű robotja újabb mérföldkövet ért el:[32]
*„2025 márciusában a cocobo autonóm biztonsági robotunk Japánban elsőként kapott tanúsítványt arra, hogy közutakon és nyílt közterületeken, beleértve az éjszakai használatot is, alkalmazható legyen. Ennek eredményeként a cocobo jelenleg előfizetőink telephelyein olyan járőrútvonalakon közlekedik, amelyek közutakat és nyílt közterületeket is érintenek, és a jövőben az alkalmazási területek bővülésére számítunk."*

[27] KMBC 9, 'Kansas City shopping center credits 600-pound AI security robot with crime reduction' https://www.youtube.com/watch?v=17vllaR3N1w accessed 2026.01.04.
[28] Global Times, 'Chinese researchers develop amphibious spherical robot assisting in police patrol in E.China's Zhejiang' https://www.globaltimes.cn/page/202412/1324773.shtml accessed 2026.01.04.
[29] CGTN, 'Sichuan police deploy robot officers to assist in traffic control' https://www.youtube.com/watch?v=uCFb5f4KAEw accessed 2026.01.04.
[30] Boston Dynamics, 'Atlas® and beyond: the world's most dynamic robots' https://bostondynamics.com/atlas/ accessed 2026.01.04.
[31] Csete Róbert, 'Mesterséges Intelligencia a kriminalisztikában – Alkalmazások és tapasztalatok. Szakdolgozat.' (Pécsi Tudományegyetem 2024) 14-16.
[32] SECOM, 'SECOM REPORT 2025' https://assets.minkabu.jp/news/article_media_content/urn%3Anewsml%3Atdnet.info%3A20251104587269/140120251104587269.pdf?utm_ accessed 2026.01.04.

A robot emellett szolgálatot teljesít az Osaka Expón és a Narita Nemzetközi Repülőtéren is.[33] MI-alapú rendszerrel összekötött kameráival képes földön fekvő embereket, gyanús tárgyakat és személyeket, továbbá bármilyen, a járőrútvonalon megjelenő akadályt azonosítani. Autonóm módon ellenőrzi a kijelölt területet, majd észlelés esetén jelzést küld a biztonsági személyzet központjába. Ezzel megmarad az „ember a folyamatban" és nagy eséllyel elkerülhetővé válik a hibás döntéshozatal.

A tanulmány szempontjából azonban cocobónak van egy rendkívül fontos további tulajdonsága is. 5G kapcsolaton keresztül összeköthető a védendő épület biztonsági és kamera rendszerével, felvonóival. Ez lehetővé teszi, hogy a már telepített biztonsági infrastruktúra részévé váljon. És hogy miért olyan „rendkívül fontos" ez? A választ szinte az összes biztonsági robotot, robotkutyát és drónt alkalmazó és gyártó szereplő indokolásában megtaláljuk…

## III. Integrált biztonsági rendszerek

A válasz: munkaerőhiány. A jóléti társadalmakat sújtó egyik legfenyegetőbb probléma. A SECOM 2025-ös jelentése a következőket fogalmazza meg:[34]

*„Mivel a munkaképes korú népesség csökkenése várhatóan tovább súlyosbítja a munkaerőhiányt a biztonsági szolgáltatások ágazatában, azon dolgozunk, hogy a digitális transzformáció (DX) eszközeinek alkalmazásával növeljük a biztonsági járőrözés hatékonyságát és pontosságát. Ennek részeként a helyhez kötött biztonsági őröket hordható eszközökkel látjuk el, bevetjük a cocobo autonóm biztonsági robotot, valamint továbbfejlesztjük az MI-alapú kamerák alkalmazását, […] Meggyőződésünk, hogy ezeknek a technológiáknak a kihasználása hatékony együttműködést és integrációt tesz lehetővé: az MI és a robotok azokat a feladatokat látják el, amelyekre kifejezetten alkalmasak, míg a biztonsági őrök azokra az összetettebb tevékenységekre összpontosíthatnak, amelyek emberi mérlegelést és magas szintű, gondos ügyfélkiszolgálást igényelnek. Ez kulcsszerepet játszik egy új, valódi értéket teremtő biztonsági szolgáltatási korszak megvalósításában."*

A Knigthscope így fogalmaz:[35]

*„A Knightscope egy erősen széttagolt amerikai közbiztonsági piacon működik, amelyet az automatizált és mesterséges intelligencián alapuló megoldások iránti erős kereslet jellemez, a növekvő munkaerőköltségek, a biztonsági személyzet hiánya és a kihívásokkal teli bűnözési helyzet miatt."*



[33] SECOM TV, **セキュリティロボット「cocobo」紹介動画｜セコム** https://www.youtube.com/watch?v=FNEE8NViwT4 accessed 2026.01.04.

[34] SECOM, 'SECOM REPORT 2025' https://assets.minkabu.jp/news/article_media_content/urn%3Anewsml%3Atdnet.info%3A20251104587269/14012025110458726 9.pdf?utm_ accessed 2026.01.04.

[35] United States Securities and Exchange Commission, 'Annual Report – Knightscope Inc.' https://www.sec.gov/Archives/edgar/data/1600983/000110465925069628/tm2521071d2_ars.pdf?utm_ accessed 2026.01.04.

Az Europol 2025. november 6. napján megjelent - The Unmanned Future(s) (A személyzet nélküli/autonóm jövő(k)) című - jelentése[36] (a továbbiakban: Europol-jelentés) is említi, hogy az elöregedő társadalmak és az autonóm rendszerek és robotika fejlődése, a fizikai MI (physical AI) jelensége mind azt eredményezik, hogy a mindennapi élet minden szegletére kiterjednek majd a félautonóm vagy autonóm technológiai megoldások. A jelentés főbb megállapításai között olvashatjuk az „eszközöktől a kollektíváig" pontot, miszerint:
*„A rendvédelmi szerveknek különböző ember nélküli rendszerekből álló, kölcsönösen együttműködő csapatokat kell létrehozniuk, amelyek képesek a küldetések értelmezésére és az emberekkel való közös munkára. Ez kiterjesztené a műveleti lehetőségeket, egyesítené a különböző képességeket, és új, hatékony módokon fejlesztené a hagyományos rendvédelmi műveleteket."*

A tanulmány korábbi fejezeteiben vizsgált technológiai megoldások mind rendelkezésünkre állnak. Láthattuk, hogy akár önmagukban képesek javítani a bűnügyi statisztikákon, mérsékelni vagy teljesen magukra hárítani az embereket fenyegető veszélyeket és optimalizálni a rendvédelmi tevékenységeket. A cocobo mellett a K5-ös robot is integrálható egy nagyobb léptékű biztonsági rendszerbe. A Knightscope a hardver – szoftver – ember hármasára alapozza integrált rendszerét.[37]

A legalsóbb szinten a járőröző autonóm biztonsági robotok és a biztonsági szempontokat figyelembevéve kihelyezett vészhelyzeti kommunikációs eszközök találhatók. Elsődleges szempont az adatgyűjtés és elrettentés.



A középső szinten helyezkedik el a Knightscope Biztonsági Műveleti Központ és a Knightscope Vészhelyzeti Igazgatási Rendszer. E rendszerek lehetővé teszik a hardveres szintről beérkező jelzések valós idejű fogadását és összehangolt kezelését.

A legfelső szinten kapott helyet a Kockázati és Fenyegetettségi Kitettség egység és a Knightscope Hálózati Műveleti Központ. Ezek feladata egyrészt, hogy kiküszöböljék az emberi hibákat és tehermentesítsék az alsóbb szinteket, másrészt az, hogy gondoskodjanak a rendszert alkotó egyes elemek karbantartásáról és műszaki felügyeletéről.

A vállalkozás állítása szerint így közel tízezer gépet és hálózatot látnak el az Egyesült Államokban.

Értelemszerűen nem a Knightscope rendszere az egyetlen létező vagy felvázolt rendszer, ám világosan látható, hogy a különféle rendelkezésre álló technológiai megoldások integrált biztonsági-rendvédelmi rendszerekbe terelése korántsem életszerűtlen. Ezt az irányt vetíti előre és támogatja az Europol-jelentést is.

A drónokon, robotkutyákon és biztonsági robotokon túl pedig számos olyan fejlesztést és technológiai megoldást vehetünk számba, amik hasznos elemei

[36] EUROPOL, 'The Unmanned Future(s)' https://www.europol.europa.eu/publication-events/main-reports/unmanned-futures?utm_term=unmanned-futures accessed 2026.01.04.
[37] Knightscope https://knightscope.com/ accessed 2026.01.04.

lehetnek – több esetben már azok is – ezeknek az integrált rendszereknek. Ilyen például a SoundThinking[38] bűncselekményelőrejelző (korábban PredPol) és lőfegyverekkel leadott lövések hangját észlelő rendszere (ShotSpotter), az arcfelismerő technológiával ellátott kamerarendszerek és testkamerák, a kriminalisztikai fonetikára alapuló rendszerek, az említetteken túl további félautonóm és autonóm vízi, légi, szárazföldi járművek, valamint számos más technológiai megoldás.

## IV. Összegzés

A tanulmányban bemutatott gyakorlati példák alapján megállapítható, hogy a drónok, robotkutyák és biztonsági robotok a világ számos rendőrségénél és biztonsági infrastruktúrájában fokozatosan elfoglalják kiérdemelt helyeiket. Mindeközben rohamos fejlődés jellemzi a vonatkozó tudomány- és iparágakat, amik további technológiai megoldások színrelépését eredményezhetik. Nem szabad azonban megfeledkezni az eseményeket befolyásoló egyéb tényezőkről sem. Figyelembe kell venni, hogy az országok eltérő módon kezelik a robotika és MI kérdését, nem beszélve az említett országok társadalmainak hozzáállásáról.

2025. december 11. napján Donald J. Trump, az Amerikai Egyesült Államok elnöke úgy rendelkezett[39], hogy:

*„2. szakasz: Politika: Az Egyesült Államok politikája az, hogy a mesterséges intelligencia területén fennálló globális vezető szerepét fenntartsa és tovább erősítse, egy a lehető legkisebb terhet jelentő, országos szintű MI-szabályozási keretrendszer révén."*



A cél egyértelmű. Az elnöki rendeletben is hivatkozott MI-versenyt mindenképpen az Egyesült Államoknak kell nyernie.

Az Európai Unió MI-versenyben vállalt szerepéről az Europol-jelentés - az Unió világpolitikában betöltött jelenlegi szerepéről alkotott általános véleményt megerősítve – az jósolja, hogy:[40]

*„2035-re a technológiai iparág szerkezete mélyreható átalakuláson ment keresztül: a 2020-as évek számos meghatározó MI-vállalata teljes mértékben robotikai nagyhatalommá vált. Ezek a cégek – elsősorban az Egyesült Államokban és Kelet-Ázsiában székelve – […] meghatározó szerepet töltenek be. […] A robotika többé nem önálló iparág, hanem az MI-birodalmak kiterjesztése, […] és néhány globális szereplő szoros ellenőrzése alatt áll."*

Továbbá:

*„Európa, korai ambíciói ellenére az etikus MI és a digitális szuverenitás terén, lemaradt a robotikai versenyben. Bár egyes uniós tagállamok helyi innovációs klasztereket hoztak létre, a*

[38] SoundThinking, 'Law Enforcement' https://www.soundthinking.com/law-enforcement/ accessed 2026.01.04.

[39] The White House: 'ENSURING A NATIONAL POLICY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE' https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/ accessed 2026.01.04.

[40] EUROPOL, 'The Unmanned Future(s)' https://www.europol.europa.eu/publication-events/main-reports/unmanned-futures?utm_term=unmanned-futures accessed 2026.01.04.

*kontinens továbbra is kritikusan függ a külföldi vállalatoktól a fejlett robotikai hardverek és szoftverek tekintetében. Ez a függőség sehol sem olyan látványos, mint az európai rendvédelem és közbiztonság területén."*

Érdemes tehát figyelembe venni a versenyzők stratégiáit. Míg az Egyesült Államok és Kína az első helyért vetélkednek és minden erejükkel egymást próbálják lesodorni a pályáról, addig az Öreg Kontinens az elveket[41] és technokrata túlkapások lehetőségét szem előtt tartva megkésve igyekszik a dobogóra.

A versengés azonban nem akadályozhat meg minket abban, hogy külön-külön vizsgáljuk meg a robotika, az MI-tudományok és a kriminalisztika legújabb vívmányait, hiszen egyre inkább úgy tűnik, hogy az autonóm rendszereket integráló biztonsági-rendvédelmi rendszerek jelentik a bűnüldözés jövőjét.

## NYILATKOZATOK

**Összeférhetetlenség**
A szerző nem jelentett összeférhetetlenséget.

**Támogatások és finanszírozás**
A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.



**Adathozzáférhetőség**
A cikkhez nem tartozik adatkészlet.

**Mesterséges intelligencia felhasználása**
Jelen cikk elkészítéséhez a szerző nem használt fel mesterségesintelligencia-rendszert.

**Szerzői hozzájárulások (CRediT)**
Conceptualization; Methodology; Investigation; Formal analysis; Resources; Data curation; Writing – Original Draft; Writing – Review & Editing.

[41] Adrián Fábián, Emese Fazekasné Pál, Balázs Hohmann and Eszter Rózsás, 'Atipikus hatósági tevékenység és döntéshozatal, különös tekintettel az új közigazgatási rendtartás: The Atypical Activity and Decision-Making of the Administrative Authorities with Special Regard to the New Act on the Administrative Proceedings' (2017) 1 *Pro Publico Bono: Magyar Közigazgatás* 4, 29.
Balázs Hohmann, 'A mesterséges intelligencia közigazgatási hatósági eljárásban való alkalmazhatósága a tisztességes eljáráshoz való jog tükrében' in Bernát Török and Zsolt Ződi (eds), *A mesterséges intelligencia szabályozási kihívásai: Tanulmányok a mesterséges intelligencia és a jog határterületeiről* (Ludovika Egyetemi Kiadó 2021) 403.

# THE IMPACT OF TECHNOLOGICAL DEVELOPMENTS ON HUMAN RIGHTS: LESSONS FROM THE EUROPEAN UNION AND RECOMMENDATIONS FOR VIETNAM

*Pham Thi Minh Trang*
*Lecturer, Commercial Department, Ho Chi Minh City University of Law (Vietnam)*
*Doctorate Student, Doctoral School of Law, University of Pécs (Hungary)*
*Corresponding address: ptmtrang@hcmulaw.edu.vn*
*ORCID: 0009-0002-2291-2724*

**DOI: 10.47272/KIKPhD.2025.3.3**

**ABSTRACT**
The development of technology is acknowledged as a great achievement of human beings. It facilitates connection and globalization, but also supports socio-economic development. Technology, particularly the existence of Artificial Intelligence, enhances convenience in daily life and promotes more efficient methods of working and conducting business. However, rapid technological growth may cause the legal framework to fall behind and pose challenges to the fundamental rights and values of human beings. This paper examines Vietnam's current legal framework for human rights protection, as well as its practice of implementation. It also analyzes the General Data Protection Regulation, the Artificial Intelligence Act, and other relevant European Union documents to gain experience from the European Union. Then, this paper will propose some recommendations to address gaps in Vietnamese regulations and strengthen the protection of human rights.



**KEYWORDS**
Personal data; biometric identifier; freedom of expression; technological development; non-discrimination.

**ARTICLE HISTORY**
SUBMITTED 19 Dec 2025 | REVISED 21 Dec 2025 | ACCEPTED 28 Dec 2025

## I. Introduction

The technologies are rapidly developing and significantly impacting all sectors of socio-economic, as well as human rights. In Vietnam, the internet was introduced officially in 1997. With its sharp development, it has become a core infrastructure for the country's digital transformation.[1] As of January 2024, Vietnam had 78.44 million internet users, accounting for 79.1% of the population, with an average daily usage time of nearly seven hours.[2] Additionally, social media platforms have experienced steady growth since 2008. They have created a vast network that connects to the lives and work of most people. In particular, the rapid and explosive development of AI has marked a turning point that drives economic and social progress. Technical developments have facilitated a comfortable and convenient life for human beings, especially with the advent of the Internet, social media platforms, Artificial Intelligence (AI), and Big Data.

However, while the technological developments bring a variety of advantages, they also pose high risks of violating human rights. In Vietnam, personal data leaks are becoming increasingly frequent and complex. According to the 2024 Survey of the National Cybersecurity Association, there are 73.99% of users consider their data leaks occur because they provide personal information when shopping online, and 62.13% attribute the leaks to sharing information on social media.[3] As a result, fraud has become increasingly prevalent, particularly through phone calls and bank account hacking. Meanwhile, personal data, particularly biometric identifiers, is integrated into most personal devices and application accounts. If cybercrimes or hacker attacks occupy this data, the damage is unimaginable.



On the other hand, cyberspace has gradually evolved into an online environment where people can connect and share with one another worldwide. Therefore, establishing legal rules to safeguard the right to freedom of expression on cyberspace has become a prerequisite and an urgent obligation in the digital era. These rules help prevent violations of privacy and protect the legitimate interests of individuals and organizations, while also creating favourable conditions for building a democratic society. Moreover, while AI offers significant benefits for the socio-economic aspects, it also poses high risks to the protection of human rights.

[1] Tran Xuan Tien, 'Artificial Intelligence: Challenges to the Legal Profession in the New Era' (2024) Vietnam Lawyer Journal https://lsvn.vn/cong-nghe-ai-thach-thuc-doi-voi-nghe-luat-trong-thoi-dai-moi-a149640.html accessed 12 October 2025

[2] 'Vietnam's Internet: Thirty Years of Remarkable Growth' (*Ministry of Science and Technology*, 27 December 2024) https://mst.gov.vn/internet-viet-nam-ba-muoi-nam-phat-trien-than-toc-19724122712285863 8.htm accessed 14 October 2025

[3] Duy Anh, 'In 2024, the personal data of more than 66% of Internet users was used without authorization' (*Vietnam Lawyer Journal*, 2024) https://lsvn.vn/du-lieu-ca-nhan-cua-hon-66-nguoi-dung-internet-bi-su-dung-trai-phep-trong-nam-2024-a151492.html accessed 14 October 2025

Especially, AI discrimination has occurred when some AI systems produce biased output data or make unfair decisions, which negatively affect individuals and groups of people.

Therefore, this paper will focus on addressing three key issues, including: the right to personal data protection, the right to freedom of expression in Cyberspace, and Artificial Intelligence and the fight against Discrimination. This paper analyzes and evaluates the current regulatory framework in Vietnam and examines relevant EU regulations to draw lessons from the EU's experience. It then clarifies the challenges to protecting human rights that arise in the context of legal implementation during an era of rapid technological developments. This paper also provides some recommendations to strengthen the protection level of human rights in Vietnam's legal framework.

## II. The Right to Personal Data Protection

### *1. Personal Data and Current Practices in Viet Nam*

In the technology era, where technology has become an integral part of our daily lives,[4] people increasingly use and interact on digital platforms. It gives rise to the storage and sharing of personal data in a digital environment. In Vietnam, several websites for online shopping, e-marketplaces (such as Shopee, Tiki, TikTok Shop, and Lazada), social media platforms, and applications related to transportation, food services, or other utilities collect and store a huge amount of personal data. Moreover, in the process of building a digital society, the Ministry of Justice affirmed that personal data of more than two-thirds of the population is being posted, collected, stored, and shared online in various forms and at different levels of detail.[5] In the meantime, personal data has become a valuable resource for economic activities with high commercial value in this period.



'Personal data' means any information relating to an identified or identifiable natural person. According to the General Data Protection Regulation (GDPR)[6], it may include information that directly or indirectly identifies a natural person, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1)). Under

[4] Vlona Pollozhani Shehu and Visar Shehu, 'Human rights in the technology era – Protection of data rights' (2023) 7(2) European Journal of Economics, Law and Social Sciences 1. https://doi.org/10.2478/ejels-2023-0001

[5] Ministry of Justice of Viet Nam, 'The Proposal to Develop the Law on Personal Data Protection' (2024) https://datafiles.chinhphu.vn/cpp/files/duthaovbpl/2024/Thang09/1.totrinhluatbaovedulieucanhan.doc accessed 10 January 2026

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)

Vietnamese regulations, personal data is divided into two types: basic personal data and sensitive personal data. According to Article 2(2) of the Law on Personal Data Protection 2025, 'Basic personal data'[7] refers to personal data reflecting common personal details and background information, frequently used in transactions and social relations. Article 2(3) of this Law also provides a definition of 'Sensitive personal data'[8]. It refers to personal data associated with individuals' privacy rights that, if infringed on, directly affect the legitimate rights and benefits of agencies and organizations.

Notably, among these types of personal data, biometric data is a form of sensitive data that is increasingly used in the technological development era, providing several effective solutions in various areas, particularly in identification methods. The right to identity is a fundamental right, recognized by Article 6 of the Universal Declaration of Human Rights (UDHR): *"Everyone has the right to recognition everywhere as a person before the law"*. Accordingly, each country has its own mechanisms for identifying its citizens. In traditional methods, the identification of a person can be recognized by a classical photograph on a passport or ID card. However, with advances in technology, biometric identifiers have become new methods that are gradually replacing these older forms of identification due to their convenience, sophistication, and high level of accuracy. Biometric technologies describe the range of tools and procedures used to analyse, measure and record one or more of these unique human characteristics.[9] They collect and generate biometric data, which includes unique physical and biometric characteristics of an individual to identify them. These data are increasingly sophisticated and measurable parameters.



In the legal sector and management of the State, the 2023 Law Identification provides a definition of "biometric identifiers"[10]. There are some popular types of biometric identifiers, including fingerprint, facial scan, voice

[7] Basic personal data was specified by the Government by giving a list of basic personal data. It may include: a name, date of birth, date of death or disappearance, gender, place of birth, place of residence, contact address, nationality, personal image, phone number, personal identification number, passport number, driver's license number, marital status, information on family relationships, information on a person's digital accounts, etc. (Article 3 of Decree 365/2025/ND-CP Detailed Regulations on the Implementation of Certain Articles and Measures for the Enforcement of the Law on Personal Data Protection)

[8] Sensitive personal data includes information revealing racial or ethnic origin, political or religious beliefs, private or family life, health status, biometric or genetic data, sexual life or orientation, criminal records, location data, login credentials and identification documents, financial or banking information, etc. (Article 4 of Decree 365/2025/ND-CP)

[9] Robert Brumnik and Iztok Podbregar, 'Biometric Technology and Human Rights' (2010) 7(1) US-China Law Review 1.

[10] Article 3(3) of the 2023 Law Identification, "*Biometric identifiers"* mean biometric or biological characteristics that are distinctive and stable of a person, used to identify and distinguish such person from another one

recognition, iris recognition, and DNA[11]. These serve as effective tools and are suitable for a wide range of purposes. Vietnamese citizens from the age of 14 must carry out procedures for the issuance of an ID card.[12] As a result, the authorities will collect personal information such as name, address, date of birth, gender, and biometric identifiers as specified in Article 18 of this Law. Thus, citizens have the obligation to provide personal information and biometric identifiers, except for DNA and voice[13]. Personal data is collected and stored in the identification database, which can be extracted by State agencies, political organizations, and socio-political organizations, depending on performing their functions and tasks. The extraction of information from the database is strictly regulated, as it requires the consent of both the competent authority and the individuals whose personal data are involved.

At the same time, in the banking sector, beyond basic personal data, biometric technologies have been widely applied in recent years. Under Circular No 17/2024/TT-NHNN on Opening and Use of Checking Account at Payment Service Provider (came into force from July 1, 2024), biometric information of account holders, in the case of individual customers, or of legal representatives, in the case of organizational customers, must be collected when checking accounts are opened electronically at banks and foreign bank branches. With customers who already have accounts, cash withdrawal and e-transactions made via checking accounts are only allowed when personal identification documents and biometric information are cross-checked. Therefore, e-wallets or integrated payment accounts on e-marketplaces or websites must undergo biometric verification to continue to be used.



In the above situations, personal data is compulsorily collected in accordance with legal regulations; however, in practice, it is also collected and used by numerous other actors for various purposes and at different levels. It is evident that there is an imbalance in the way information technology is used. Many people have a mindset that they are willing to trade personal and private information for technological convenience. Besides, during the training and utility of AI, people also provided a lot of important personal information. Therefore, a segment of the population is ready to disclose personal information on digital platforms without full consideration of the potential risks. In other words, the awareness of most Vietnamese users regarding personal data protection remains relatively low. Meanwhile, the potential for data leaks on these online platforms and applications is significantly high because existing security measures are inadequate, and measures to combat data abuse are also not clearly defined. With the vast scope and diverse

[11] Article 15 of the 2023 Law Identification No 26/2023/QH15 dated November 27, 2023

[12] Article 19 of the 2023 Law Identification

[13] Because both are voluntarily provided by each citizen or collected by the criminal proceedings agency or the supervisory agency of persons against whom administrative measures are taken

levels of data collection in cyberspace while cybercrimes, online fraudulent schemes, and deepfake identity fraud have become increasingly sophisticated.

### *2. Regulations on the protection of personal data*

Regarding regulations on the protection of personal data, from an international perspective, the GDPR is one of the pioneering instruments regulating the protection of personal data and biometric data; however, this legal field is still relatively new in Vietnam. The first legal instrument that directly regulated the protection of personal data was promulgated by the Government in 2023, Decree No. 13/2023/ND-CP on the Protection of Personal Data. This Decree provides a fundamental legal basis for protecting personal data amid the rapid development and application of biometric technologies. It sets out a legal basis for enhancing the management of the collection, processing, and transfer of personal data, as well as mitigating risks during this period. Although this Decree draws on many experiences of the GDPR, differences in legal systems, economic conditions, social factors, existing precedents on personal data protection[14], and limited legislative experience in this field have resulted in several limitations in the initial Decree.

During this period, many companies, particularly service businesses, collect customers' personal data and allow third-party partners to access such data with lax requirements or safeguards. As a result, third parties can transfer or trade personal data to other entities. The purchasing and selling of personal data has become increasingly complex through numerous sophisticated methods. However, the violations have not been specified, which impairs the effectiveness of law enforcement. Civil, administrative, and criminal sanctions are either insufficiently deterrent or, in some cases, have not yet been established.



Therefore, on June 26, 2025, the legislative body (the National Assembly) further developed and refined numerous new elements for the promulgation of the first Law on Personal Data Protection. This law took effect on January 1, 2026, replacing Decree 13/2023/ND-CP, and aims to strengthen the level of protection of personal data. It is a foundational legal instrument at the statutory level on the protection of personal data in general, as well as biometric data in particular. Moreover, this Law is further detailed in Decree No. 356/2025/ND-CP, which also took effect on the same date. It provides detailed regulations on the implementation of certain Articles and measures for the enforcement of the Law on Personal Data Protection.

[14] Ministry of Justice of Viet Nam, the Proposal to Develop the Law on Personal Data Protection (2024) https://datafiles.chinhphu.vn/cpp/files/duthaovbpl/2024/Thang09/1.totrinhluatbaovedulieucanhan.doc accessed 10 January 2026

According to this Law, the legal framework for protecting personal data is strengthened more than in the previous Decree. It can be proved by the following points:

*First*, previously, the protection of personal data was recognized primarily as a set of rights, but it lacked effective enforcement mechanisms. However, the Law on Personal Data Protection establishes detailed regulations, such as the methods, duration, and necessary procedures to give effect to the protection of human rights. For example, the consent and withdrawal of consent of the data subject are set out in Articles 9, 10, and 19 of this Law. Accordingly, to process personal data, the data subject has to give consent in a clear and specific manner,[15] except for the processing of some cases, such as to protect the life, health, and legitimate rights of the personal data subject; to respond to emergencies to national security; to serve the state management according to the law, etc. Besides, this law lays down the conditions for withdrawal of consent, the legal mechanisms, as well as the responsibility of the controlling party.

Moreover, the Law also supplements the detailed regulations on the handling of violations of personal data protection. In other words, as a result of the GDPR experience, the Law establishes stricter sanctions for such violations. Depending on the nature, severity, and consequences of the violation, organizations or individuals may be subject to civil, administrative, or criminal liability. Notably, illegal trading in personal data and unlawful cross-border transfers of personal data may be subject to administrative fines amounting to a significant proportion of revenue, including fines of up to 10 times the revenue obtained from the violation or up to 5% of total revenue, respectively.



*Secondly*, the provision on notices of violations against personal data protection regulations is regulated for the first time, aiming to promptly detect and remedy violations (Article 23 of the Law on Personal Data Protection). Specifically, when the data controller, the data processor, or a third party detects violations of personal data protection regulations that may harm national defence, security, social order, or public safety, or infringe upon the life, health, honour, dignity, or property of the personal data subject, they shall notify the personal data protection authority within 72 hours of detecting such violations. They shall also promptly inform relevant parties to prevent or mitigate damage.

In addition, agencies, organizations, and individuals may actively participate in protecting personal data. Where they detect personal data being

[15] Methods for obtaining the consent of data subjects shall ensure verifiability, including the ability to identify that consent has been given by the data subject, as well as the time and content of such consent. Consent may be obtained in writing; through recorded telephone calls; via consent messages sent by mobile text message; through email, websites, platforms, or applications equipped with technical mechanisms for obtaining consent; or by other appropriate methods that can be printed or reproduced in written form, including electronic documents or other verifiable formats. (Decree No. 356/2025/ND-CP).

processed for improper purposes or in violation of agreed terms, or where the rights of data subjects are not ensured, they may report such violations to the competent authorities. Moreover, the responsibilities of these entities are governed by this Law. Enhanced cooperation among these entities, with clearly defined deadlines, can promote voluntary compliance of relevant subjects.

*Thirdly*, the Law also supplements specific regulations governing foundation sectors, as well as emerging fields. For example, regarding social media platforms and online communication services, they have rapidly expanded their user bases and have become potential sources of personal data leakage. According to Article 29 of the Law on Personal Data Protection, providers of social media and online communication services are required to offer a "Do Not Track" option or to track user activities only with the data subject's consent. Furthermore, eavesdropping, wiretapping, recording calls, or reading text messages without the consent of the personal data subject is strictly prohibited. Notably, service providers are not permitted to request images or videos containing all or part of personal identification documents for account verification purposes. Besides, confidentiality policies and the methods of collecting, using, and sharing personal data must be clearly disclosed and explained to users.

On the other hand, Article 31 of this Law sets out strict standards for the protection of personal location data and biometric data. In particular, it clarifies the prohibition of unlawful location tracking and defines the obligations of mobile application platform providers when collecting or using personal location data. Regarding biometric data, the collection and processing have to enhance the adoption of physical confidentiality measures for their biometric data transmission and storage devices; restrict rights to access to biometric data, and establish monitoring systems to prevent and detect acts of infringement.



Furthermore, personal data in environments such as big data, artificial intelligence (AI), blockchain, virtual spaces, and cloud computing is regulated to provide guidance on data processing, clarify risk levels for the application of appropriate personal data protection measures, and ensure compliance with ethical standards and Vietnamese customs (Article 30).

In short, the Law on Personal Data Protection lays down the rights of personal data subjects and the obligations of controllers and processors, and revises the sanctions applicable to violations of personal data protection rules. Although the rights provided under Vietnamese Law remain more limited than those under the GDPR, this Law represents a significant step forward. For example, the Law does not recognize the right to data portability, which under the GDPR allows data subjects to receive their personal data and transmit it directly from one controller

to another.[16] However, it cannot be denied that Vietnamese Law has drawn lessons from the GDPR and has been considerably improved compared to Decree No. 13/2023/ND-CP, such as data protection impact assessments (Articles 21 and 22 of the Law) and the obligation to notify personal data breaches to the supervisory authority (Article 23). Therefore, the effective implementation of this Law, together with the strengthening of human rights protection, requires a clear roadmap for further development and refinement. This journey also needs to take into account Vietnam's socio-economic conditions in order to progressively raise the level of personal data protection.

## III. The Right to Freedom of Expression in Cyberspace

One of the equally important issues in the protection of human rights during the technology era is cybersecurity and the right to freedom of expression. On the one hand, freedom of expression is a fundamental right of every human being. This right constitutes essential foundations for democracy, rule of law, peace, stability, sustainable, inclusive development and participation in public affairs.[17] Under Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, this right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. Alongside the exercise of this right, individuals must also fulfill certain duties and responsibilities to ensure the interests of the State and other persons. These obligations serve the interests of national security, territorial integrity, and public safety; the prevention of disorder or crime; the protection of health or morals; the safeguarding of the reputation or rights of others; the prevention of the disclosure of confidential information; and the preservation of the authority and impartiality of the judiciary.



On the other hand, cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[18] In cyberspace, a communication system and information processing are created where people's activities are not limited by space and time. In other words, cyberspace or the Internet is where shared information and social interactions occur, and it has

[16] Andreas Nicolas Häuselmann, 'EU privacy and data protection law applied to AI: Unveiling the legal problems for individuals', Doctoral thesis, Universiteit Leiden (2024) https://core.ac.uk/download/612047553.pdf accessed 21 January 2026

[17] The European Union, 'EU Guidelines on Freedom of Expression Online and Offline' https://www.eeas.europa.eu/sites/default/files/09_hr_guidelines_expression_en.pdf accessed 3 November 2025

[18] U. M. Mbanaso and E.S. Dandaura, 'The Cyberspace: Redefining A New World' (2015) 17(3) IOSR Journal of Computer Engineering 18. https://doi.org/10.9790/0661-17361724

become a central part of modern life.[19] It has transformed various aspects of society, including commerce, entertainment, and communication.[20] In early 2025, Vietnam had 79.8 million internet users, with 78.8% of the population connected online.[21] According to the 2024 Report of the Ministry of Information and Communications, there are approximately 110 million Vietnamese people using social networks. Zalo records 76.5 million monthly active users, Facebook has 72 million users, and TikTok reaches 67 million users, etc.[22] Moreover, the Government and relevant authorities have official websites and social media accounts with large followings. It plays an effective disseminating information and conducting public communication.

However, the more development and expansion of cyberspace, the greater the risk it is to cyber-attacks, thereby posing greater risks to users and information systems. Threats to cybersecurity can include computer viruses, spam, identity theft, data breaches, denial of service attacks, and cybercrime.[23] The EU and some other countries have declared the issue of cybersecurity, and specifically cyber attacks against their governments and citizens, as a national security threat and have developed national cybersecurity strategies or initiatives.[24]

Moreover, sharing of personal information, daily activities, thoughts, feelings, or status updates has become common, even gradually replacing traditional communication methods. Because digital platforms involve a wide range and are difficult to control, individuals may intentionally or unintentionally disclose sensitive information. In certain cases, such platforms can be misused as tools to act against the State or to disseminate content that harms, insults, or defames other individuals or organizations. The abuse of freedom of expression, especially on social networks to spread misinformation and cause public confusion, has become increasingly common. In many cases, such acts aim to undermine the government or attack other entities. Given the speed at which information spreads and the powerful influence



[19] Kafi Mahmud, Ehashan Ahmed, Zaedul Islam, Baki Billah, Biplob Banarjee, KariulIslam, 'Freedom of Expression in Cyberspace: Society, Law and its Effects in Bangladesh's Perspective' (2024) 44(4) Library Progress International 843.

[20] Ibid. 844.

[21] DataReportal, Vietnam Digital Overview Report 2025 https://cleverads.vn/blog/digital/ accessed 5 November 2025

[22] Minh Sơn, 'Which social media platform is the most widely used in Vietnam?' (*Ministry of Science and Technology*, 29 December 2024) https://mst.gov.vn/mang-xa-hoi-nao-duoc-nhieu-nguoi-dung-nhat-tai-viet-nam-19725010716061544 6.htm accessed 2 November 2025

[23] Carolina Rossini And Natalie Green, 'Cybersecurity and Human Rights' (*gp-digital*, 2015) https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf accessed November 15, 2025

[24] Minh Sơn, 'Which social media platform is the most widely used in Vietnam?' (*Ministry of Science and Technology*, 29 December 2024) https://mst.gov.vn/mang-xa-hoi-nao-duoc-nhieu-nguoi-dung-nhat-tai-viet-nam-19725010716061544 6.htm accessed 2 November 2025

of social media, this can cause significant harm, including damage to reputation, dignity, and public trust.

Therefore, it is an essential factor in ensuring a safe digital environment and mitigating potential threats. This is a precondition for the implementation of the right to freedom of expression, as well as ensuring social security. Drawing on the EU's experience, the EU will pay particular attention to key issues to promote and protect the right to freedom of expression.

One of these is combating violence, persecution, harassment, and intimidation of individuals, including journalists and other media actors.[25] Under a judgment of the European Court, a higher level of protection for journalistic reporting on matters of public interest, also recognising "the right of the public to be properly informed" about matters of interest for society.[26] Accordingly, any actions that infringe upon or threaten individuals for exercising their right to freedom of expression must be publicly condemned. The EU calls on all Member States to prevent violence against journalists and other media actors, and to promote the exchange of awareness-raising initiatives and training measures aimed at preventing attacks.

Besides, enhance programmes for exchanging opinions and expressions with all relevant stakeholders, such as law enforcement officers, the judiciary, civil society, politicians, human rights defenders, lawyers, security forces, academics, and religious or cultural agencies[27], to strengthen the protection and promotion of the right to freedom of expression. Member States research and improve the Law, aiming to limit excessive interference by authorities in the exercise of the right to freedom of expression when such expression does not infringe upon the rights of others. The authorities encourage whistleblowers to report abuse of these rights to violate the interests or privacy of individuals, organizations. On the other hand, requirements for creating and verifying social media accounts serve as an effective tool to reduce risks and help build a safer online environment where individuals can exercise their right to freedom of expression. Alongside this, strong account



[25] The European Union, 'EU Guidelines on Freedom of Expression Online and Offline' https://www.eeas.europa.eu/sites/default/files/09_hr_guidelines_expression_en.pdf accessed 3 November 2025

[26] Dirk Voorhoof, 'The Right to Freedom of Expression and Information under the European Human Rights System: Towards a more Transparent Democratic Society' (Working Papers of RSCAS 2014/12 Robert Schuman Centre for Advanced Studies Centre for Media Pluralism and Media Freedom) https://cadmus.eui.eu/server/api/core/bitstreams/c6386959-9781-5723-a94c-932056331aeb/content accessed 10 November 2025

Balázs Hohmann, 'Integrity Advisors and the Development of Administrative Communication Culture' (2019) 4(1) European Journal of Multidisciplinary Studies https://doi.org/10.26417/ejms-2019.v4i1-527

[27] The European Union, 'EU Guidelines on Freedom of Expression Online and Offline' https://www.eeas.europa.eu/sites/default/files/09_hr_guidelines_expression_en.pdf accessed 3 November 2025

verification measures must be paired with robust security systems to protect users against hackers and other cyberattacks.

Vietnam adopted the Cybersecurity Law in 2018. It aims to ensure that activities in cyberspace do not harm national security, public order, or the lawful rights and interests of any organization or individual. This Law establishes fundamental rules that aim to enhance the safety and security of activities carried out in cyberspace. At the same time, Chapter III of this Law sets out rules on the prevention and actions against cybersecurity violations and regulates cybersecurity protection activities to create a secure internet environment. It also assures human resources for cybersecurity protection. However, these regulations are general and provide overall guidance; they do not specify particular violations or establish sanctions for such violations. Until 2022, Decree No. 53/2022/ND-CP on Elaborating Some Articles of The Law on Cybersecurity of Vietnam was issued and partially addressed some difficulties in implementation by authorities.

Thus, information in cyberspace will be monitored by competent authorities to promptly address fake news, misinformation, defamatory content, and the disclosure of others' private information, etc. However, this may lead to restrictions on the right to freedom of expression, especially when the State seeks to shape public opinion. For example, one dimension of this freedom is the right to seek and receive information. In certain situations, the State may apply the Cybersecurity Law as a means to restrict the public's access to information. As a result, individuals may be unable to obtain sufficient and accurate information or to gain a comprehensive understanding of an issue. In some cases, persons who expose shortcomings within the governmental system or criticize particular State policies may be blocked or even sanctioned. Such practices may infringe the freedom to hold opinions or to convey information that is essential for ensuring a democratic and rule of law principle. These actions may stem from vested interests or from attempts by individuals or groups in positions of authority to conceal wrongdoing.



## IV. Artificial Intelligence and Non-discrimination

The fourth industrial revolution introduced disruptive technologies like big data and artificial intelligence[28]. These show the most remarkable achievements in modern technological progress. AI, in particular, possesses faster and more accurate analysis capabilities than humans. It can process huge amounts of data in a short time to examine, analyze, and generate effective recommendations. Moreover, AI has professional language skills that enable it to understand and translate into many

[28] Zhisheng Chen, 'Ethics and Discrimination in Artificial Intelligence - Enabled Recruitment Practices', Humanities and Social Sciences Communications (2023) 567. 1. https://doi.org/10.1057/s41599-023-02079-x

different languages. These features make AI an intelligent and versatile tool that supports human activities across virtually all sectors.

AI systems have had a significant impact on most aspects of life, particularly as generative AI is capable of producing new data outputs that shape subsequent processes. Meanwhile, the nature of generative AI relies on collected data and the use of algorithms, as well as user-provided prompts, to generate answers, predictions, new products, or proposed solutions. Its outputs depend largely on the quality, accuracy, and diversity of the data on which it was trained, as well as the way prompts are formulated. Therefore, in some cases, AI systems may produce results that are biased or discriminatory because there are various subjective and objective reasons for this. It rises to harmful bias and discrimination with risks to individuals, communities, or societies. These issues may stem from incomplete or inaccurate training data, unclear prompts, the subjective intentions of those who train the AI, or errors in training data processing.

Researchers and technologists have repeatedly demonstrated that algorithmic systems can produce discriminatory outputs.[29] Practically, when AI systems are used in employment management or in the recruitment and selection of personnel, their decisions can seriously affect the right to work of individuals and even their future career prospects. For example, AI applications used by Amazon as a recruiting tool have been found to discriminate based on gender.[30] Besides, when AI systems are used as supporting tools in education or in the workplace, faulty algorithms that generate biased or discriminatory outputs can lead to unfair treatment and create misguided tendencies for a specific group of people. Furthermore, a system in the United States used to assess the risk of reoffending within the criminal justice system was found to discriminate on the basis of race. This system predicted that people of color may reoffend almost twice compared to white persons.[31] In short, any negative impacts are likely to broaden in scale and scope.



In Vietnam, there is no independent document regulating discrimination in technology and AI. This issue is combined in several legal sectors. First, Article 16 of the 2013 Constitution of the Socialist Republic of Vietnam provides that all people are equal before the law. No one is subject to discriminatory treatment in political, civil, economic, cultural, or social life. Moreover, Article 26 claims that male and female citizens have equal rights in all fields. The State shall adopt policies

[29] Chiraag Bains, 'The legal doctrine that will be key to preventing AI discrimination' (*Brooking*, 13 September 2024) https://www.brookings.edu/articles/the-legal-doctrine-that-will-be-key-to-preventing-ai-discrimination/ accessed 05 November 2025

[30] More referrence: Jeffrey Dastin, 'Insight - Amazon scraps secret AI recruiting tool that showed bias against women' https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/ accessed 15 October 2025.

[31] Bach Duong, 'The impact of artificial intelligence' (*Nhandan,* 28 March 2024) https://nhandan.vn/tac-dong-cua-tri-tue-nhan-tao-post802055.html accessed 10 November 2025

to guarantee the right to and opportunities for gender equality. The State, society, and family shall create the conditions for women to develop comprehensively and to advance their role in society. All gender discrimination acts are prohibited. This is reclaimed in the 2006 Law on Gender Equality, which aims to highlight and implement this rule in specific fields, such as politics, economy, labour, education, and technology. The 2019 Labor Code, the 2010 Law on Persons with disabilities, the 2019 Education Law, etc, also provide rules on prohibiting discrimination.

Overall, the current regulations are quite general and fragmented across multiple legal domains and specialized legislative areas. When identifying AI-driven discrimination and implementing measures to combat it, there is no unified definition, and regulations are governed by many legal domains. This leads to different interpretations among authorities or even a shifting of responsibility among them. This fragment creates a challenge in effectively enforcing these regulations.

Meanwhile, in the EU, 2024 marked a significant milestone with the adoption of the world's first AI Act. This Act provides a solid foundation when creating a uniform legal framework for the development and use of AI systems in the Union. As Recital 56 of this Law, if AI systems are improperly designed and used, these may be intrusive and may violate the right not to be discriminated against and perpetuate historical patterns of discrimination, for example, against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. Therefore, the AI Act requires providers to implement appropriate safeguards to protect the fundamental rights and to comply with all applicable conditions for high-risk AI systems. These obligations aim to ensure the quick detection of bias and discrimination. On the other hand, training, validation, and testing data are vital elements in the development of high-risk AI systems, and therefore, they must be subject to strict data governance and management practices. Therefore, under Article 10 of this Act, one of these is an examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights, or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations.



Thus, the AI Act sets out a classification framework for AI systems in order to ensure that risk-appropriate governance measures are applied. It also establishes specific requirements for high-risk AI systems to mitigate misuse and to reduce bias and discrimination. With risk prevention methods and the clarification of obligations of providers, this Act facilitates the robust development of AI and ensures cybersecurity. It is not only a precondition for building trust among developers and users, but also an effective support tool for socio-economic development.

In conclusion, the remarkable development of technology has transformed cyberspace into an integral part of human life. The number of activities that take place within cyberspace or are closely connected to it is increasing. Therefore, the protection of human rights can not be limited to the physical world but must also be expanded into cyberspace. From this perspective, transparency may serve as a cross-cutting guarantee of rights protection, since it connects the accessibility of legal norms, the accountability of public authorities and the effective exercise of individual rights.[32] Vietnam and many other countries have been proactively developing and implementing specific regulations to protect human rights in technological development. Meanwhile, the EU has established a solid and comprehensive legal framework for human rights protection. Studying the EU's experience and assessing Vietnam's current legal framework will help identify appropriate pathways to improve human rights protection. This plays a vital role in the country's development and integration process.

## STATEMENTS

### Disclosure statement

No potential conflict of interest was reported by the author.



### Funding

The author received no financial support for the research, authorship, or publication of this article.

### Data deposition and availability

There is no data set associated with the study. No data deposition was required for this study.

### Use of Artificial Intelligence

The author did not use any artificial intelligence system in the preparation of this article.

### Author contributions (CRediT)

Conceptualization; Methodology; Investigation; Formal analysis; Resources; Data curation; Writing – Original Draft; Writing – Review & Editing.

[32] Balázs Hohmann, *Az átláthatóság értelmezése és követelményrendszere a közigazgatási hatósági eljárások tükrében* [The Interpretation and Requirements of Transparency in Administrative Authority Proceedings] (Novissima Kiadó 2022) 271.

# KEEP ENERGY PRICES DOWN, INDUSTRY IN, COMPETITION HIGH, MANIPULATION OUT EUROPE – A DECADE WITH THE REGULATION ON THE WHOLESALE ENERGY MARKET INTEGRITY AND TRANSPARENCY (REMIT)

*Attila Nyikos*
*Director, Office for Supported Research Groups, HUN-REN TKI (Hungary)*
*Doctorate Student, Doctoral School of Law, University of Pécs (Hungary)*
*Corresponding address: nyikosdr@gmail.com*
*ORCID: 0009-0007-1106-2978*

**DOI: 10.47272/KIKPhD.2025.3.4**

**ABSTRACT**
Next year we are going to mark the 15th year of application of the EU Regulation No 1227/2011, designed to ensure integrity and transparency in the wholesale energy markets. It is high time to address the legal experiences of it, and its effect to the market, how it achieved partly or entirely its declared goals, to detect, deter and sanction market manipuation and insider trading, in order to better protect EU citizens and enterprises from market abuse. This article tries to sum up REMITs working experiences and enlighten its functioning through real life cases from its past present.



**KEYWORDS**
REMIT; insider trading; market manipulation; wholesale energy products.

**ARTICLE HISTORY**
SUBMITTED 19 Oct 2025 | REVISED 29 Nov 2025 | ACCEPTED 28 Dec 2025

## I. Introduction

Before getting into details, it is worth walking through the reader, on what were exactly the key elements, of REMIT, which on the analogy of stock market trading rules, started to regulate wholesale energy trading in Europe. [1] Key elements were: banning insider trading (Art 3), market manipulation (Art 5) mandatory publication of inside information (Art 4) transaction reporting (Art 8) market surveillance by ACER (Art 7).

The 2024 reform - Regulation (EU) 2024/1106 of the European Parliament and of the Council of 11 April 2024 amending Regulations (EU) No 1227/2011 and (EU) 2019/942 as regards improving the Union's protection against market manipulation on the wholesale energy market - expanded scope (storage, financial instruments), strengthened ACER investigatory powers for cross-border cases, and algorithmic trading oversight.[2]

The enforcement framework of REMIT is quite simple, ACER at EU level monitors data, flags anomalies, coordinates national authorities, and takes actions as necessary, in cooperation with NRAs. But its maine role is to hand down cases to the National Regulatory Authorities, NRA-as to further investigate and sanction cases discovered by ACER.[3] It is mostly the National Regulatory Authorities (NRAs) which take action and enforce sanctions, fine violators, sometimes issue warnings.



Enforcement powers vary across member states. In the Czech Republic, energy insider trade is a crime, so investigators of an NRA go out to house search accompanied by the Police and K9 unit dogs, and the result of their investigation will land on the desk of a state prosecutor. In Hungary it is not a criminal offence yet (differently from crimes of the financial market [4]) The table below demonstrates,

[1] Rushkovskyi, M. and Rasshyvalov, D., 'European Remit Regulation As The Latest Determinant Of Corporate Risk Management Strategies In Energy Sector' (2022) 3 (1) Green, Blue and Digital Economy Journal 40-46. https://doi.org/10.30525/2661-5169/2022-1-7

[2] Ratliff, John and Mariia Shulha, 'Amendments to REMIT in 2024.' EU Energy Law Volume X: Energy Market Manipulation and Insider Trading Law in Europe–REMIT (Edward Elgar Publishing 2025) 877-904. https://doi.org/10.4337/9789077644225.00035

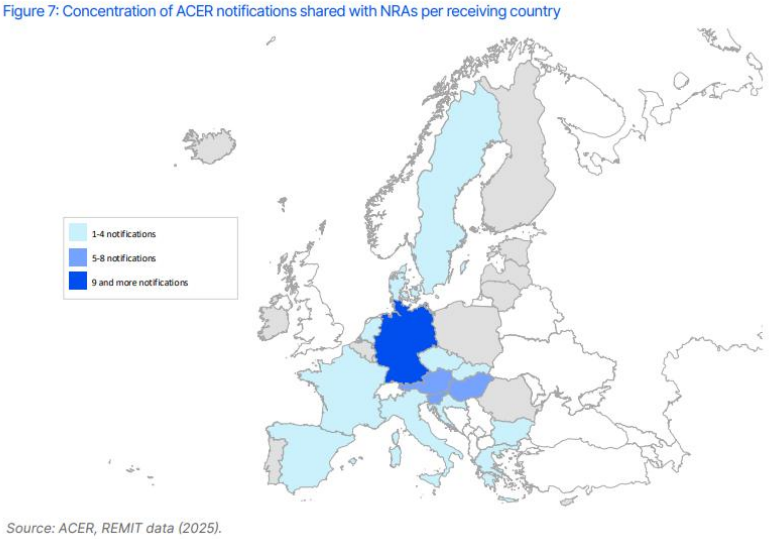
Berceanu, Ionuț Bogdan, Mihaela Victoriţa Cărăuşan and Alina Zorzoană. 'The Regulation of Market Manipulation in the EU Energy Sector: Doctrinal Analysis of REMIT II's Sanctioning Framework.' (2025) 14(5) Laws 61. https://doi.org/10.3390/laws14050061

[3] Godin, Jean-Theodore, Manon Polet and Arthur JAMAR DE BOLSÉE, 'Implementing REMIT: What a Legal Analysis Tells about the (Regulatory) Role of ACER.' (2018) 9(2) European Journal of Risk Regulation 192-207. https://doi.org/10.1017/err.2018.17

[4] „Hungarian Criminal Code: Insider Trading Section „*410§ (1) Any person who*
*a) uses inside information to conclude a transaction, give an order to conclude a transaction, withdraw or modify an order, record, withdraw or modify an offer, in his own name or in the name of another person, in a financial instrument affected by the inside information, or who, with regard to the inside information in his possession, invites or compels another person or persons to conclude a transaction, give, withdraw or modify an order to conclude a transaction, record, withdraw or modify an offer, shall be punished by imprisonment for a term not exceeding three years*."

that the Central European area, and bidding zones therein are the playground of a vivid commodity trading, but also suspicious market manouvers[5].

**Figure 1: Concentration of ACER notification shared with NRAs per receiving country.**




Source: https://www.acer.europa.eu/sites/default/files/REMIT/REMIT%20Reports%20and%20Recommendations/REMIT%20Quarterly/REMITQuarterly_Q1_2025_2.0.pdf

What are the major types of market abuse, that REMIT covers? From cases and ACER now the 6th time updated guidances we can say that there are five major types of them.

The first is capacity hoarding/withholding – which is in other words trading against itself to block capacity. By definition it is the acquisition of all or decisive part of the available transmission capacity (ATC) without using it or without using it effectively. ACER gave out its first Guidance on it in 2018 [6], where

[5]https://www.acer.europa.eu/sites/default/files/REMIT/REMIT%20Reports%20and%20Recommendations/REMIT%20Quarterly/REMITQuarterly_Q1_2025_2.0.pdf

[6]https://www.acer.europa.eu/sites/default/files/REMIT/Guidance%20on%20REMIT%20Application/ACER%20Guidance%20on%20REMIT/Guidance%20Note%20-%20Transmission%20Capacity%20Hoarding.pdf

it described in great detail, what is the nature of this type of market abuse. From the Guidance we know that „The transmission capacity is considered used effectively when it is used to fulfil a legitimate need of the market participant driven by the (expected) supply and demand of electricity in the different bidding zones". It makes a great difference what was the reason for you to buy this capacity. You buy it to prevent others from using it or to create or enhance a price difference between two bidding zones, or there was a real need for it?. It is also important to know, that intraday capacity markets work on the first come first served basis. So if you are quick to react, you may buy the decisive part of the available transmission capacity, ATC. There are two ways of buying capacity: one can actively match its own order or the system will match you when a new capacity occurs. It is though very important for traders to prove real capacity need at the given time. ACER has got triggering indicators on that. First there must be price difference between the bidding zones. Second: what was the portion of the acquired capacity. Third: time difference between the transactions. Fourth: if there was direct or indirect reversal, use of wash trades, applying inconsistent orders. Today NRA-s and ACER have a great experience on judging these small, but important differences.

Withholding can be two types. Phisical or commercial. Physical is to not offering or limiting without justifyable cause available electricity or gas production, storage or transportation capacity on the market by market participant with the relative ability to influence the price or the interplay of supply and demand of a wholesale energy product. Economic or commercial is offering available generation capacity but at prices which are known to be above the market price and do not reflect the marginal cost (including opportunity cost) of the market participant's asset, which results in the related wholesale energy product not being traded or related asset not being dispatched.[7]



Wash trading is in other words – self-matching orders. In wash trading the seller and the buyer is the same person, in most cases hidden behind seemingly different market participants. It works as that one is selling and buying its own energy product from itself, and the false perception of trade is urging prices up. This practice applies different accounts or brokers to create a false impression of market activiy. It will mislead honest brokers about the demand for the product (high trading volume and liquidity) and will inflate its price.

Marking the close / layering / spoofing – placing fake orders to influence price or settlement. Under that method a market patricipant issues a false order to influence other market participants' behaviour, e.g. by creating the impression that there is a stronger selling or buying interest at decreasing/increasing price levels than there actually is (non-genuine orders are issued in order to enter into transactions at better conditions regarding price or volume on the other side) So

[7] Zani, A., Spisto, A., Vitiello, S., Grisi, P., Siface, D., Gelmini, A. and Geracitano, A., 'Case studies analysis of REMIT regulation' in *2020 17th International Conference on the European Energy Market (EEM)* (IEEE 2020) 1-5. https://doi.org/10.1109/EEM49802.2020.9221989

transaction(s) on the other side of the book will occur within a period that allows the false orders to influence the behaviour of bystander market participants, than miraculously the false orders are cancelled shortly after the entering into one or multiple transactions on the other side of the order book by the real players[8].

Marking the close is a specialty: it is buying or selling wholesale energy products deliberately at the close of the market in with a view to modify the exchange's daily closing price (on any individual trading day or on particular dates such as future/option expiry dates or quarterly/annual portfolio or index reference/valuation points). It is mostly done with minimal tradable amounts.

False or misleading information – it is misrepresenting supply/demand to manipulate balancing markets. This is done by a market participant posting information via internet, electronic or printed press or issuing a press release which contains false or misleading statements about a wholesale energy product which is admitted to trading on an organized market (Exchange), where the disseminating person knows, or ought to know, that the information is false or misleading, so it is willfully done.[9]

For example, when a TSO provides incorrect information on the transmission capacities on the interconnector to the dayahead auction or submitting by a producer of balancing mechanism to TSO false or misleading notifications which falsely estimate expected generation for a time period (mostly at the high demand periods,when prices are high) in order to induce the TSO to pay participant to generate or submitting to TSO misleading (inflated) information on the minimum amount of power that generation plant can supply. [10]



Insider trading is also one of the most common infractions of the REMIT. It can only be committed by persons with insider information. These persons shall not use that information for buying or selling wholesaleenergy products, disclose that information to anybody not needed to know, or recommending or inducing another person to buy or sell.

Failure to disclose inside information means that market participants shall publicly disclose in an effective and timely manner inside information which they possess in respect of business or facilities which the market participant concerned.

Such information must include relevant information to the capacity and use of facilities for production, storage, consumption or transmission of electricity

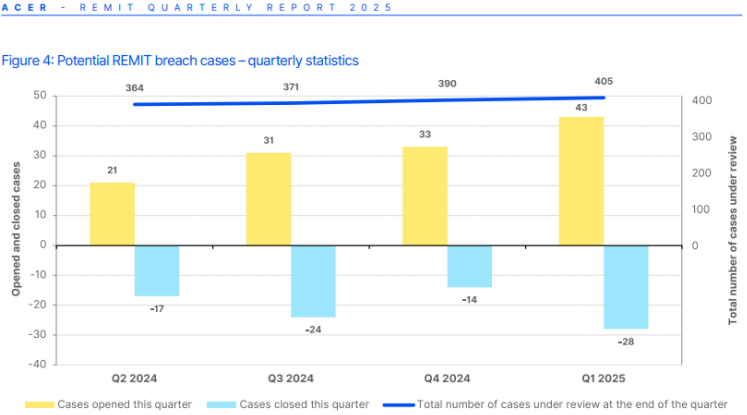
[8]https://www.acer.europa.eu/sites/default/files/REMIT/Guidance%20on%20REMIT%20Application/ACER%20Guidance%20on%20REMIT/Guidance%20Note_Layering%20v7.0%20-%20Final%20published.pdf

[9] Ratliff, J., and Nteve, M., 'Market Manipulation Under Remit-Key Concepts And Developing Enforcement Practice' (2020) European Energy & Climate Journal (Claeys & Casteels BV) 9. https://doi.org/10.4337/eecj.2020.02-03.07

[10] Ratliff, John, 'REMIT in the United Kingdom' *EU Energy Law Volume X: Energy Market Manipulation and Insider Trading Law in Europe–REMIT*. (Edward Elgar Publishing 2025) 695-729. https://doi.org/10.4337/9789077644225.00031

or natural gas or related to the capacity and use of LNG facilities, including planned or unplanned unavailability of these facilities, as all these information have got a direct effect to the market, to trade. But there can be cases, exceptionally for delay. In such cases ACER and the NRA must be informed, with reasoning. The table below demonstrates the constant growth of REMIT investigation cases, accumulated during pas periods before 2024, and handled this year[11].

**Figure 2: Potential REMIT breach cases – quarterly statistics.**




Source: https://www.acer.europa.eu/sites/default/files/REMIT/REMIT%20Reports%20and%20Recommendations/REMIT%20Quarterly/REMITQuarterly_Q1_2025_2.0.pdf

## II. Case Studies

### 1. Case Study: Energi Danmark – Capacity Hoarding and Market Manipulation

Energi Danmark,[12] a major Danish energy trading company, was investigated and sanctioned for a case of market manipulation involving cross-border capacity hoarding and wash trading. This was one of the first fully adjudicated and public REMIT enforcement actions in Denmark, providing a precedent for how such

[11] https://www.acer.europa.eu/sites/default/files/REMIT/REMIT%20Reports%20and%20Recommendations/REMIT%20Quarterly/REMITQuarterly_Q1_2025_2.0.pdf

[12] https://forsyningstilsynet.dk/nyheder/2018/dec/energi-danmark-pays-fine-for-manipulation-with-the-electricity-market

conduct is interpreted and penalized under REMIT (EU Regulation No. 1227/2011).[13]

The manipulation occurred on 29 July 2015, during a time of routine operations in the Nordic electricity markets. The Nordic power market is highly interconnected, with cross-border transmission playing a critical role in price formation. Transmission system operators (TSOs) allocate cross-zonal capacity for electricity traders, who may profit from arbitraging price differences between bidding zones (e.g., between Denmark and Sweden).

Energi Danmark engaged in a wash trading scheme involving matched buy and sell orders across interconnectors. Specifically, artificial self-trading: The company placed identical buy and sell orders for electricity across two bidding zones, effectively trading with itself at the same price and volume.

It was also blocking cross-border capacity: These fictitious transactions occupied capacity on the DK1-SE3 (Western Denmark–Sweden) interconnector, preventing other market participants from accessing the transmission line. By using capacity without genuine economic interest in the trades, Energi Danmark manipulated the price spread between the two zones, profiting indirectly through other open positions.

This behavior was qualified as market manipulation under Article 5 of REMIT, and more specifically the blueprint example outlined in ACER's Guidance on Market Manipulation (e.g., capacity hoarding, wash trades, and the creation of a misleading impression of supply and demand).



The Danish national regulator, Energitilsynet (now part of the Danish Utility Regulator), received the initial report and referred the matter to ACER for technical analysis. ACER's REMIT surveillance system, which continuously monitors reported trade data (via Registered Reporting Mechanisms, or RRMs), flagged unusual patterns suggesting circular trades. The investigation revealed that the trading pattern could not be explained by legitimate hedging or portfolio optimization purposes.

Energi Danmark's first offense occured in 2015, and the company was fined in December 2018, for DKK 750,000 (100 000EUR) capacity hoarding and wash trading on 10 occasions, than on 3 January 2020, Energi Danmark was again fined for DKK 380,000 (approx. €50,900) by the Danish Utility Regulator.

The company made a profit of DKK 80,693 (approx. €10,800) from the manipulation.The regulator found Energi Danmark in breach of Article 5 of REMIT and relevant Danish legislation implementing the regulation. It is also

[13] Lakić, E., Jeriha, J., Medved, T., Vućić, D., Topić, D. and Knežević, G., 'Unveiling market manipulation in EU energy markets-Insights from ACER enforcement cases' in *2025 21st International Conference on the European Energy Market (EEM)* (IEEE 2025) 1-6. https://doi.org/10.1109/EEM64765.2025.11050114

important to mention that the recurrence raised concerns about the deterrent effect of fines at the time in Denmark.[14]

This was one of the first cases to demonstrate how REMIT can be used to target subtle forms of cross-border manipulation that distort price signals.

Very important is the ending of the case. Energi Danmark did not appeal it. They accepted the fines, and the criminal case was closed at the prosecutors desk.

The case clarified that self-matching cross-border trades, even without direct profit from the wash itself, can constitute market manipulation if they hinder fair access or influence prices. It also marked a transition in Danish enforcement from purely administrative penalties to active use of REMIT's market integrity provisions. The Danish regulator published the rationale for its decision, providing transparency in a field where many cases remain undisclosed or settled privately.[15] But, it had one major consequence for the future: The penalty-to-profit ratio (less than 5:1) raised concerns about the adequacy of enforcement deterrence. Critics argued that fines should be proportional not only to the gain but also to the potential market impact and recurrence.

Following this case and others like it, ACER and national regulators have since pushed for stronger penalties, more consistent enforcement across member states, and the creation of public registers of sanctions to increase transparency.

The Energi Danmark case illustrates how even modest manipulations in the electricity market can disrupt pricing efficiency and harm market confidence. It also reveals the challenges regulators face in detecting and deterring abuses in a rapidly evolving and technically complex trading environment.



## 2. Case Study: Spain – Gesternova and Axpo Iberia (2022)[16] Stuffing and Marking the Close in Wholesale Energy Markets

Between 30 September and 30 December 2022, the Spanish national regulator, CNMC, discovered that two major participants in the intraday electricity market (the non-interruptible intraday segment of the Iberian electricity grid) manipulated order books on cross-border interconnectors with France by using quote stuffing tactics: rapidly placing and canceling orders to obstruct fair competition and secure priority in transaction execution. [17] What is quote stuffing? The latest version (2024) of

[14] Ratliff, J., & Nteve, M., 'Market Manipulation Under Remit-Key Concepts And Developing Enforcement Practice' (2020) *European Energy & Climate Journal (Claeys & Casteels BV)* 9.

[15] Balázs Hohmann, 'The Interpretation of Transparency from the Legal Point of View' in Tamás Haffner (ed), *4th Youth in Europe Conference – Proceedings* (Sopianae Cultural Association 2018)
Balázs Hohmann, 'The Principles and Fundamental Requirements of the Transparency on the Public Administrative Proceedings' in Suresh P (ed), *Proceedings of the IIER International Conference*, Dubai, UAE (International Institute of Engineers and Researchers 2019)

[16] https://www.cnmc.es/sites/default/files/5698012.pdf

[17] Bernabeu Villena, J., 'Análisis prospectivo de la demanda energética residencial e implementación de medidas de adaptación al riesgo de shock de precios' (2023)

ACER Guidance on the Application of REMIT says at its section 6.3.2. (315) „i) Quote stuffing: entering a large number of orders to trade and/or cancellations and/or updates to orders to trade so as to create uncertainty for other participants, slowing down their process, and/or to camouflage one's own strategy;"

It could only work by AI, by computer robots. An algorithmic order bombardment was used by Gesternova S.A. and Axpo Iberia to flood the intraday market with false sell orders. These non-genuine orders—and their cancellations—slowed down or prevented other participants from securing advantageous queue positions. And as markets across France and Spain link at specified times, quotes placed earlier in the queue executed first, it enabled Gesternova and Axpo to capture favorable trades across the border.

„During the months of October, November, and December 2022, the broker GESTERNOVA S.A. had placed a high number of new bid submissions before the opening of trading in the non-interruptible intraday for the next-day contracts (which occurs at 3:10:00 p.m.). These submissions were invalid and were intended solely to monopolize the bid processing queue to be the first to have a valid bid in the next-day contracts (hereinafter D+1). According to the market rules in force at that time, "Hibernated bids will be reactivated in the order in which they arrive on the Market Operator's Trading Platform" (Rule 46.2.7). Therefore, competition among agents occurred around 3:10 PM until March 3, 2023, since the objective was to have priority in reactivating bids after the third session of the intraday market auction (session closing at 9:50 PM) for execution with purchase bids for the D+1 product (at 10:00 PM). Specifically, by cornering the bid processing queue, the agent sought to position itself first in the entry order to execute its sell bids by attacking purchase orders external to the Iberian market, while the bids were reactivated based on the order in which they arrived at OMIE's trading platform, known as LTS (Local Trading Solution), and therefore, their validation." (excerpt translation from the original Spanish decision)



„The proven facts show that between September 30 and December 30, 2022,16 GESTERNOVA manipulated the organized electricity market by bombarding the processing queue with a high volume of non-genuine bids or bids with no intention of execution—which were rejected by the system (97.8% of GESTERNOVA's total bids during the investigation period). The sole intention was to monopolize the bid processing queue, preventing other agents' orders from being placed before its own or interspersed with its own, thus allowing GESTERNOVA to obtain an advantageous position over other agents in the D+1 product bid. The LTS bid bombardment strategy allowed GESTERNOVA to

https://www.acer.europa.eu/sites/default/files/documents/Other%20Documents/6.1st_Edition_ACER_Guidance.pdf

position 21.6% of the bids validated as of 3:10:00 PM for the D+1 product at the top of the MIC bid book."

The CNMC cited breach of Article 5 REMIT, specifically concerning the issuance of false or misleading signals about supply via deceptive order book behavior.

In the end, Gesternova was fined by CNMC to 6 million EUR, and Axpo Iberia received a 1.5 million EUR sanction fine[18] - underscoring that quote stuffing, though subtle, carries major consequences when network integrity is jeopardized."

Spain has got no natural gas on its European territory. Never had. All its natural gas is imported in the form of liquid natural gas aka LNG into LNG terminals, where, after regasification it is transmitted to the national pipeline system and mostly used for balancing electricity power production in CCGT gas power plants. We can say, that natural gas trade is directly connected to the electricity market. That is why this gas market manipulation case had so serious consequences to the committing company, Enérgya VM Gestión de Energía in 2022.

The essence of the case is that the spanish energy regulatory authority, the National Commission on Markets and Competition (CNMC) has fined Enérgya VM Gestión de Energía, S.L.U. one million euros for manipulating the organised gas market (MIBGAS) between 1 September and 31 December 2022 **(SNC/DE/002/23).**



The authority found that its „operation was illegitimately aimed at raising the market price to an artificial level by inserting purchase offers that he had no intention of matching. In 32 trading sessions, it submitted purchase offers at high prices in the last seven seconds of trading. These were not modifications of previous offers, which it was trying to execute in the last seconds of the negotiation, nor did they attack the most competitive sale offer at that time in the negotiation system, since it introduced them at a slightly lower price – in some sessions only €0.02/MWh below – to prevent them from being matched.

In addition, these purchase offers were entered for a volume of energy much lower than the volume of the rest of the purchase offers of Enérgya VM Gestión de Energía, S.L.U. in the same market session. The objective was to reduce the economic impact of the high-priced offers in the event that they had been matched and, in some of the sessions, against economic logic, since it introduced them at a higher price than the last transaction executed by the agent as a selling counterparty for the same product and in the same trading session.

None of these bids were matched, but the final price of the D+1 product was altered on several occasions. Thus, in 27 of these 30 trading sessions of the D+1 product, the purchase offer placed by ENÉRGYA, in the final seconds of trading, reduced the bid-ask spread sufficiently so that the midpoint between the price of its purchase offer and that of the most competitive sale offer defined the

[18] https://www.cnmc.es/prensa/multa-axpoiberia-manipular-mercado-intradiario

final price of the D+1 product for those trading sessions (condition 2 of the methodology for calculating the final daily price, in force at that time, in accordance with market rules)

The introduction of false or misleading signals about the supply, demand or price of a wholesale energy product, as well as the pricing of a wholesale energy product at an artificial level, correspond to manipulative behaviour or attempted market manipulation, which infringes Article 5 of REMIT.

The infringement committed by Enérgya VM Gestión de Energía, S.L.U. was classified as serious, in accordance with the provisions of Article 110 u) of Law 34/1998, of 7 October, on the Hydrocarbons Sector."[19]

It is interesting also to hear the defence of the company, as it is in the decision of CNMC: „ Regarding the legality of the transaction, ENÉRGYA alleges: 1) that only the 32 market sessions belonging to the group of unmatched bids were analyzed, instead of the 57 bids made in the last minute of the session during the period investigated, of which 14 were matched, which indicates the lack of legality of the conduct; 2) that MIBGAS in no case warned it that its conduct could constitute market manipulation; and 3) that the fact of placing bids in the last minutes/seconds of the session cannot be classified as unlawful, as the regulations permit it, and the price set was not artificial."

This argumentation could not stand the investigation of CNMC, so the company received one of the greatest fines in the history of REMIT in Spain. CNMC concluded that Enérgya had artificially set prices in breach of Article 5(2)(a)(ii) of REMIT.



The broader context of the regulatory response has a combined meaning. These cases reveal two distinct but complementary manipulation techniques: 1. quote stuffing distorts order book dynamics in intraday electricity and 2. marking the close manipulates settlement prices in gas markets for next day opening. Both are exploit high-frequency market mechanics, and both were caught and sanctioned via vigilant regulatory AI bot monitoring tools including real-time trade reporting and algorithmic detection.

Impacts beyond fines for the Spanis market were to give priority to algorithmic fairness, and markets tightened systems to prevent queue manipulation and last-second order abuse. The regulators all around Europe strengthened real-time monitoring and enforcement via trade reporters and cross-border data-sharing.

Since trading is done electronically, it is mostly no human traders watching monitors all days, but AI bots, specially developed tools that do the trade. So what are the takeaways of the present case: One, that algorithmic manipulation is real, even micro-second tactics can distort prices and undermine market trust. Two, that

[19] https://www.cnmc.es/ és 5511280.pdf

systemic conduct draws scrutiny, and regulators target behavioral patterns spanning multiple sessions rather than isolated trades. Thre, that transparency in methodology gives a clear guidance (e.g., ACER's REMIT editions) aids detection and legal justification. Four, is that the magnitude of the penalties does matter, and multi-million-euro fines ensure penalties outweigh potential gains or cost of reform, with persuasive force.

The spanis case exemplifies modern energy market abuse: subtle, tech-driven, and systematic. CNMC's response—rooted in REMIT and ACER guidance—illustrates how regulators now patrol both the microstructure of markets and the final price formation process. These cases serve as benchmarks for enforcement agencies across the EU aiming to preserve integrity[20] in increasingly fast-paced trading environments.

### 3. The UK case (from the time they were member of the EU)(OFGEMs decision was issued on the 25th of Marc 2020)

In winter 2016, InterGen (UK) Ltd along with its affiliates Coryton, Rocksavage, and Spalding submitted false or misleading physical notifications and stable export limits to the National Grid's Electricity System Operator (ESO) during the critical evening demand period known as the "Darkness Peak".[21]

They indicated the plants would not generate during peak hours, prompting ESO to pay them to remain available ("extended on"). Once secured, InterGen reversed that signal, showing they would generate. They also inflated output limits to increase the ESO's required minimum purchase volumes.



As OFGEM stated later on in its decision „The Authority found that InterGen breached Article 5 of REMIT on 31 October 2016, 7 November 2016, 8 November 2016 and 15 November 2016 ("the Four Days"). InterGen UK; Coryton; Rocksavage; and Spalding are liable for this breach. The Authority also found that Coryton, Rocksavage and Spalding breached SLC 5.1 of their Electricity Generation Licence. Coryton, Rocksavage and Spalding are liable for this breach." [22]

„The Authority found that InterGen engaged in market manipulation to exploit Great Britain's Balancing Mechanism, a Wholesale Energy Market. InterGen submitted false or misleading physical notifications which misrepresented its best estimate of expected generation for particular time periods. Physical notifications inform the system operator (ESO) whether or not a power plant will generate

[20] Balázs Hohmann, 'Integrity Advisors and the Development of Administrative Communication Culture' (2019) 4(1) European Journal of Multidisciplinary Studies https://doi.org/10.26417/ejms-2019.v4i1-527

[21] Ratliff, J., 'REMIT in the United Kingdom' in *EU Energy Law Volume X: Energy Market Manipulation and Insider Trading Law in Europe–REMIT* (Edward Elgar Publishing 2025) 695-729. https://doi.org/10.4337/9789077644225.00031

[22]https://www.ofgem.gov.uk/sites/default/files/docs/2020/04/final_notice_regarding_the_imposition_of_a_financial_penalty_under_regulation_38_1_and_38_5_of_the_electricity_and_gas_market_integrity_and_transparency_enforcement_etc._regulations_2013.pdf

electricity over an interval of time. The submission of misleading physical notifications led to the manipulation of the market from which InterGen derived profits. InterGen also, on several occasions submitted false or misleading signals to the ESO on the power plants' operational characteristics ("Dynamic Parameters") by submitting false or misleading Stable export limits. This was done with a view to achieving even higher revenues for the power plants within the balancing mechanism."[23]

„InterGen's staff sent the ESO false or misleading physical notifications that indicated that they would not be generating at the high demand periods ("Darkness Peaks") in order to induce the ESO to pay it to generate. Once InterGen's staff executed this tactic, they would then submit updated information (through revised Physical notifications) to the ESO showing that, contrary to the earlier information, the power stations would actually be generating through the Darkness Peak period."

„InterGen disseminated false or misleading data on its supply of power for the Darkness Peak in order to be "extended on" (i.e. paid to generate) during the day (in particular during the hours leading up to the Darkness Peak) for large sums of money in the balancing mechanism." stated by OFGEM, and follows as it is: „ Therefore InterGen contravened Article 5 by: issuing an order to trade in wholesale energy products by submitting bid offer pairs on each of the four days. A bid offer pair is an offer to either generate less or generate more electricity for delivery into the balancing mechanism; submitting, on each of the four days, false / misleading physical notifications, and on occasion, a false / misleading stable export limit, all of which the bid offer pair employed as fictitious device; and that fictitious device gave, or was likely to give, false or misleading signals regarding the supply of wholesale energy products; and in submitting said false / misleading physical notifications and, on several occasions,stable export limits, disseminated information which gave or was likely to give false or misleading signals as to the supply of, demand for, or price of wholesale energy products and that it knew, or ought to have known, that that information was false or misleading."



„Coryton, Rocksavage and Spalding also breached standard licence condition of their electricity generation licences because the dynamic parameters they submitted did not reflect their true operating characteristics as required, failing to use reasonable endeavours to ensure that the data held by the ESO was accurate at all times."

„InterGen's behavior on the four fays can be summarised as follows: submitting physical notifications, which misrepresented their best estimate of expected generation for particular time periods. Physical notifications inform the ESO whether or not a power plant will generate electricity over an interval of time.

[23] op.cit.

InterGen's traders sent the ESO false or misleading physical notifications that indicated that the power stations would not be generating at all during the high demand period from around 17:00 to 19:00 ("the Darkness Peak"), when in fact they had a contracted position to meet (i.e. it had agreed to supply electricity to other parties during this period and was either required to generate to meet this obligation or to purchase electricity from the market to meet it – it had not done so)."

„InterGen submitted these misleading physical notifications in order to induce the ESO to pay the power stations to generate by purchasing the minimum level of power (i.e. a volume of power equal to the power stations' stable export limit) across the day so that the power stations would be able to generate at the Darkness Peak. This is referred to as an 'extension'. Once the 'extension' had been achieved, InterGen then re-submitted physical notifications showing that the power stations would, in fact, be generating at the Darkness Peak."

„InterGen also submitted false or misleading signals to the ESO on the power stations' operational characteristics by submitting false or misleading stable export limits (the minimum level at which a power station can, under stable conditions, generate). It did this in order to require the ESO to purchase a higher volume of power in order to "extend" the power stations on to ensure they were available at the Darkness Peak. InterGen submitted an inflated stable export limit with no underlying technical reason and purely for the purposes of commercial gain."



„Mindful of its principal objective, to protect consumers, its enforcement obligations under REMIT and the need to ensure the integrity of the electricity and gas wholesale markets, the authority considered it appropriate to impose a financial penalty of £35,000,000 (reduced to £24,500,000 for early settlement) on InterGen in respect of its contraventions of Article 5."

„In addition, the Authority has also agreed with InterGen that it will return £12,791,000 to those parties affected by InterGen's REMIT breach. The Authority has identified this figure as the market detriment. This revenue will be returned to those who suffered losses as a result of InterGen's REMIT breach via the BSUoS charge, administered by Elexon, on behalf of the ESO and market participants."

„The Authority has decided not to impose a separate financial penalty on Coryton, Rocksavage and Spalding in respect of their breach the Grid Code and SLC 5.1 as it considers that the financial penalty imposed in respect of the breach of REMIT is sufficient."

„Recognising that InterGen has admitted that it has breached Article 5 of REMIT and has agreed to settle this matter during the early settlement window, the Authority discounted the penalty by 30% in accordance with its REMIT Penalties Statement published on 23 June 2015. This settlement-oriented element of the procedure also illustrates that, alongside punitive enforcement, administrative regulatory proceedings may include consensual or cooperation-based mechanisms

that contribute to procedural efficiency and the restoration of lawful operation.[24] Accordingly, the Authority considered that it was appropriate to reduce the total financial liability due from InterGen in respect of the contraventions of Article 5 to £37,291,000."

Looking back to half a decade into the pas of REMIT, this fine was the largest-ever REMIT fine at the time — and sent a horrifyingly deterrent message to market participants.

It reinforced, that explicit misreporting to ESO, if used to distort market signals, constitutes serious market manipulation, let to immediate internal reforms at InterGen—including improved compliance, surveillance, and staff training—for avoidance of future breaches.

## 4. Case Study: Italy – ENET Gas Over-Nomination (2022)

Historical excerpts from the decision of ARERA[25]: „ With a note dated December 6, 2022 (acquired with Authority protocol 65515 of December 9,2022), Gestore dei Mercati Energetici S.p.A. (hereinafter GME) sent to the Authority, pursuant to Article 15 of the REMIT and Article 8, paragraph 2, of the Integrated Text for Monitoring the Wholesale Natural Gas Market (Annex A to Authority Resolution 631/2018/R/gas and subsequent amendments; hereinafter TIMMIG), a report of a case of suspected violation of the prohibition on market manipulation pursuant to Article 5 of the REMIT by the company ENET Energy S.A. (hereinafter: ENET or the company)."



„Specifically, this report highlighted intense physical movements (through storage re-registrations) and commercial (mirroring the physical movements, carried out in the markets managed by GME, with purchases and sales at the PSV, virtual trading point) carried out by ENET with reference to a gas day. These had significantly contributed to determining the progressive imbalance of the system, prompting the intervention of the balancing manager, Snam Rete Gas S.p.A. (hereinafter: SRG), to rebalance the system itself, through purchase offers that were mainly matched with the sale offers entered by ENET in the order book, as well as causing an increase in the gas price compared to previous prices."

„In order to acquire further information on the reported conduct, ENET was heard at the Authority's offices on January 24, 2023, and".. „the company supplemented the information stated therein. Subsequently, the Authority's offices sent a further request for information to ENET (Authority protocol 7740 of February 3, 2023), which provided the information on February 8, 2023."

Enet's defense arguments

[24] Balázs Hohmann, 'Az alternatív vitarendezés lehetőségei a közigazgatási hatósági eljárás keretében' [The Possibilities of Alternative Dispute Resolution within Administrative Authority Proceedings] (2019) 19(1) *Európai Jog: Az Európai Jogakadémia Folyóirata* 23.

[25] https://www.arera.it/fileadmin/allegati/docs/24/47-2024-S-gas.pdf

„During the hearing and in response to the communication of the preliminary findings, Enet argued that it had implemented the contested conduct to correct the erroneous purchase of a large amount of interruptible injection storage capacity for the so-called winter counterflow service offered by Stogit at the end of October 2022. More specifically, that it had erred, due to a lack of information attributable to SRG, in believing that the injection storage capacity usable with the winter counterflow service was also interruptible (and not just non-interruptible), i.e., the capacity actually used by Enet for injection.

Enet insisted that the conduct was carried out on a single day and precisely the day after SRG's clarification on the winter counterflow service, requested by Enet itself. In accordance with the best practices of operators in the sector, the company - in order to neutralize the risks arising from fluctuations in the market price in the period between the purchase of gas and its resale - regularly concludes specific hedging transactions on the market.

However, these hedge risk only in the periods identified at the time of the conclusion of the transactions themselves (which in this case was the first quarter of 2023) and, therefore, would not have been concretely useful in the specific case, which is also characterized by strong price volatility.

Therefore, in Enet's opinion, if SRG had clarified as early as October 2022 that the short-term capacity usable with the winter counterflow service was only the non-interruptible capacity, the contested conduct "would certainly not have occurred."



„In its reply to the communication of the preliminary findings, the company then disputed the statement of the Head of the proceedings according to which the recorded increase in the gas price, is attributable to the contested conduct. In support of this argument, the company highlighted how: (i) in Enet's opinion, therefore, SRG's latest intervention cannot be attributed in any way to the contested conduct, as (ii) said intervention was not relevant for the purposes of balancing the system; (iii) and all the transactions carried out by Enet, i.e., were at a price substantially aligned with the market price. If Enet had intended to profit from manipulative behavior, it could have placed offers at a higher price; (iv) the correlation between the MI prices and those of the following day's MGP in the evening hours was highest.

The operator claimed, as a justification for its conduct, that it was induced to engage in the conduct in question by a lack of information—attributable, essentially, to SRG—regarding the technical characteristics of the winter counterflow service offered by Stogit."

„As shown by the documentation acquired in the proceedings the winter counterflow service offered in October 2022 provided for the implicit assignment of delivery capacity in the period between January 1 and March 31, 2023, associated with the assignment of non-interruptible injection capacity in the period between

November 1 and December 31, 2022. Therefore, the user who had used injection capacity at the storage sites for the period November-December 2022 could have used the same delivery capacity in the period January-March 2023.

The error that Enet allegedly made was to have believed that the injection capacity can be used within the winter counterflow service (and such therefore, it is necessary to determine the implicit assignment of the same capacity for delivery in the following period, between January and March 2023), even if the capacity is interruptible (i.e. revocable) and not just non-interruptible (pursuant to Article 1 of the RAST, non-interruptible capacity is defined as "storage capacity guaranteed as non-interruptible, except in cases of force majeure or emergency" and interruptible capacity "storage capacity subject to interruptibility, with the obligation to provide advance notice by the storage company").

But this argumentation did not convince the Italian regulator, as it follows its decision by this: „The operator's argument is completely misleading. The error invoked by the company does not, in fact, refer to an element specific to the unlawful act, but to a fact completely unrelated to (and preceding) the contested conduct. In this regard, as already observed by the Head of the proceedings in the communication of the preliminary investigation findings, the alleged need to avoid potential economic losses associated with its own error of assessment - reiterated in the reply to the preliminary investigation findings - can in no way justify conduct that is contrary to the provisions in force and, in this case, to the provisions of REMIT.



Therefore, the circumstances that Enet engaged in manipulative conduct on the day it realized it had committed the above-described error and that SRG—in light of the experience gained the previous year—decided in 2023 to clarify an (actually) intrinsic characteristic of the winter counterflow service in order to achieve greater transparency among operators are completely irrelevant. Nor is the circumstance that the normal "insurance" tools the company claims to use would not have been effective in the case at hand. These are, in fact, circumstances that all pertain to the motivations underlying the contested conduct and, as such, are irrelevant to the determination of the offense in question, for which manipulative intent is not necessary.

In any case, regarding the characteristics of the contested conduct, the documents show that it involved gas overnominations in supply that were much higher than the volumes Enet injected."

At the final hearing the company attributed the amount of the overnomination to the risk of being "cut" by SRG.

Furthermore, at a certain time on the gas day in question, the company had reached equilibrium, thus resolving the alleged problem arising from the impossibility of using the winter counterflow service. But, the company continued to overnominate (in the opposite direction, i.e., by injection) for quantities well

above its actual needs in terms of handling, resulting in a significant worsening of the system imbalance, which then led to the intervention of SRG.

The arguments with which Enet criticized the authorities findings insofar as they referred to the increase in the recorded gas price, were also unfounded. In the context of this proceeding, in fact, no "anomalous price variations" were called against Enet. In any case, pursuant to Article 2, number 2, letter a), iii), market manipulation is defined as "the conclusion of any transaction orthe transmission of any order to buy or sell in wholesale energy products that uses, or attempts to use, a fictitious instrument or any other form of deception or artifice that sends, or is likely to send, false or biased signals regarding the supply, demand, or price of wholesale energy products." Therefore, the conduct in question would still be illegal, having, as already explained, sent a false signal to the market regarding the state of the system, even if SRG had not intervened or if its intervention had not resulted in an increase in the imbalance price.

Therefore, with specific reference to the observation regarding the modest size of the price variations on that day, the comparison with the price variations that occurred on the previous or following day is irrelevant for the purposes of establishing the alleged offense. For the same reason, the company's observations regarding the correlation between the prices recorded are irrelevant.

In light of all the violation was established, since the company appears to have sent misleading signals to the market, specifically, at the beginning of the day a balanced system signal (when in fact it was short, excluded ENET's improperly long position) and at the end of the day a very short system signal (when in fact it was not so short, again excluding ENET's improperly short position).



So, ENET's conduct under this provision was illicit because it violated the provisions of Article 5 of the REMIT, which prohibits market manipulation in wholesale energy markets."

So, onn 23 February 2024, ARERA (Italian NRA) imposed a €940,000 penalty on ENET Energy S.A.

As for those kind readers, who are not so much familiar with the functioning of a liquid gas market the punch line: ENET made excessively large storage nominations, requesting volumes for both injection and withdrawal that far exceeded its actual needs. These physical nominations were accompanied by corresponding exchange trades on the GME-managed PSV virtual gashub (commodity exchange in Italy)

The combined effect produced a significant imbalance in the system, prompting the TSOs (notably Snam Rete Gas) to engage in balancing actions, purchasing or selling volumes at potentially unfavorable prices. That is why ARERA determined that the inflated and sudden nominations were not aligned with ENET's real balancing needs and deliberately triggered REMIT system intervention.

This case underscored that even behind-the-scenes actions like over-nomination can constitute meaningful market manipulation. The ENET over-

nomination case serves as a leading example of non-typical manipulation detected and penalized under REMIT. By flagging a single-day misuse of storage mechanisms, ARERA delivered a strong message: manipulation isn't limited to speculative trading—it can arise from structural imbalances in operations. And regulators across Europe are prepared to enforce compliance, even via nuanced legal pathways like the "fictitious device" route.

### 5. Hungary – Gas Transport Capacity Manipulation (2022) - Prvo Plinarsko Društvo d.o.o. (PPD) vs. MEKH

The Hungarian Energy and Public Utility Regulatory Authority (HEA) issued a decision on 2 June 2023, wherein it found that Prvo Plinarsko Društvo d.o.o. (PPD) has engaged in market manipulation on the natural gas market during one of the rolling monthly capacity auctions, breaching Article 5 of the EU REMIT.[26] Article 5 says, on market manipulation that „Any engagement in, or attempt to engage in, market manipulation on wholesale energy markets shall be prohibited."

It was widely spread in energy trader circles, that HEA has fined PPD HUF 500,000,000 (approximately EUR 1.4 million). HUNGARIAN ENERGY AUTHORITY's own investigation revealed that PPD, in an "ascending clock auction", manipulated the natural gas market during the rolling monthly capacity auction, held from 17 to 26 January 2022 on the capacity product for the Austria to Hungary interconnection point for February 2022. The manipulation happened so, that PPD had registered a bid for nearly the totality of the capacity, which nobody could challenge, and in the last moment, when no other competitor was in a position to make a new valid bid, withdrew its bid.



According to HEA's decision, PPD's bidding behaviour was manipulative by maintaining its bids for almost the whole amount of the offered capacity for thirty-six bidding rounds of the auction and then in the last moment leaving the auction without actual capacity booking. By doing this, PPD raised the clearing price for the other market participants in the auction up to four and a half times of the reserve price. PPD's bidding behaviour gave false signals to the market as to the real demand of the wholesale naturalgas product in question and sticked the price of the given wholesale energy product at an abnormally high level.

On 5 July 2023, PPD submitted an administrative court action against the decision of the Hungarian Energy Authority. The case at the closure of the present writing is still pending.

This case is a clear demonstration, that market manipulation isn't limited to traditional trades—it also applies to capacity auction behavior. The substantial fine underscores that capacity auction strategies must reflect genuine interest—not

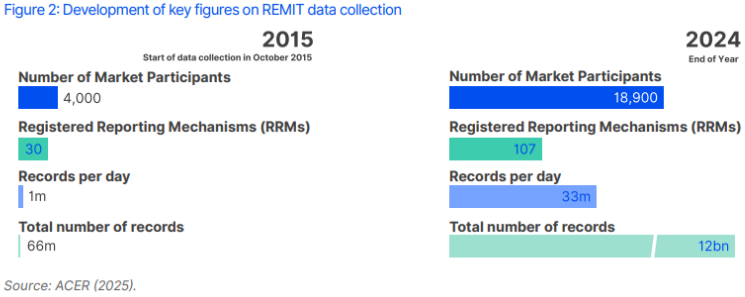
[26] REMIT breach: Hungarian regulator fines Prvo Plinarsko Društvo d.o.o. for market manipulation | www.acer.europa.eu

gaming tactics. It was the biggest fine ever issued in the history of HEA since its foundation in 1993.[27]

ACER receives and screens data from over 40 EU and EEA countries (MOU-s are concluded) and uses ARIS (ACER REMIT Information System) to aggregate order/trade data (from exchanges, brokers, TSOs, etc.), detect suspicious behaviors (e.g., cross-border arbitrage distortions), issue suspicious transaction reports (Storys) to relevant NRAs.

The table below demonstrates key numbers of REMIT data collection, in a decade. Soon the server computers of ACER have to be changed not to super computers, but to quantum computers, if the trend goes like this.

**Figure 3: Development of key figures on REMIT data collection.**






Source: https://www.acer.europa.eu/sites/default/files/REMIT/REMIT%20Reports%20and%20Recommendations/REMIT%20Quarterly/REMITQuarterly_Q1_2025_2.0.pdf

ACER algorithms flag patterns such as simultaneous buy/sell trades in neighboring markets, price/spread anomalies near interconnector deadlines, unusual transport nominations or capacity hoarding. After ACER flags a suspicious case, it alerts the NRA concerned, which starts its own investigation, or a joint investigation with other NRA-s and ACER. If the suspicion is based, they separately issue take investigations, and after the due national procedures the case ends in a fine or even criminal code consequences for the delinquants.

In the Hungarian capacity manipulation case (PPD 2022), the Croatian company was fined by the Hungarian regulator (MEKH) with ACER support. Though joint audits and inspections are legal too, as allowed under EU law, but never before were executed.

[27] https://www.acer.europa.eu/news/remit-breach-hungarian-regulator-fines-prvo-plinarsko-drustvo-doo-market-manipulation

REMIT's cross-border enforcement relies on ACER's centralized surveillance and NRA-led prosecution, with extensive data sharing, STR coordination, and procedural alignment. As markets grow more interconnected, these mechanisms are increasingly critical in identifying and punishing cross-market abuses that distort EU-wide energy pricing.

As for the future, we see, REMIT is in sky rocketing development, but what are its directions? The first is the extension of its scope to new markets (trade in LNG, hydrogen, biogas, electricity and gas storage) and new reporting obligations under REMIT II (public consultations opened this September). It envisions stronger ACER oversight, including new Investigations Department launching in 2025[28], with first cross-border cases expected in 2026. In the future, ACERs power will be greater, lets just see the possible on site investigations in cooperation with NRAs. It will make ACER the energy FBI of Europe. Market monitoring activity will be even more AI robotized with self learning capabilities and automated actions. Reporting regime improved but reporting obligations minimized. Information and data flow unified, and validated and block chain logged at every moment. So market manipulation and insider trading will not pay.

## STATEMENTS



### Disclosure statement

No potential conflict of interest was reported by the author.

### Funding

The author(s) received no financial support for the research, authorship, or publication of this article.

### Data deposition and availability

There is no data set associated with the study. No data deposition was required for this study.

### Use of Artificial Intelligence

The author(s) did not use any artificial intelligence–based system in the preparation of this article.

### Author contributions (CRediT)

Conceptualization; Methodology; Investigation; Formal analysis; Resources; Data curation; Writing – Original Draft; Writing – Review & Editing.

[28] https://www.acer.europa.eu/remit/remit-investigations