TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV

FACULTY OF LAW

ADMINISTRATIVE LAW AND PROCEDURE DEPARTMENT

&

MYKOLAS ROMERIS UNIVERSITY

FACULTY OF LAW

INSTITUTE OF PUBLIC LAW

MAKSYM BUCHYNSKYI

LEGAL REGULATION OF PUBLIC ADMINISTRATION

AND HUMAN RIGHTS

# FUNDAMENTAL RIGHTS IMPACT ASSESSMENT AS HUMAN RIGHTS PROTECTION TOOL UNDER EU AI ACT

Supervisors -

Associate Professor

PhD, Tsomenko Alina

Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)

Associate Professor

Dr. Šaltinytė, Loreta

Mykolas Romeris University (Vilnius, Lithuania)

Kyiv-Vilnius, 2026

**TABLE OF CONTENT**

**INTRODUCTION**…… 4

**LIST OF ABBREVIATIONS**……..... 13

**CHAPTER I - CONCEPTUAL AND NORMATIVE FRAMEWORK**……... 14

1.1 Legislative Development of the EU AI Act and the FRIA Obligation…….. 14

1.2 Fundamental Rights in EU Law and Their Engagement with High-Risk Artificial Intelligence…….. 19

1.3 The "Brussels Effect" and the Global Stakes of FRIA Design…….. 22

1.4 The Impact Assessment Tradition as a Human Rights Methodology…… 24

1.5 Conclusions of Chapter I……... 27

**CHAPTER II - FUNDAMENTAL RIGHTS IMPACT ASSESSMENT UNDER AI ACT: THE COMPREHENSIVE ANALYSIS**……... 29

2.1 Legal Nature, Scope and Drawbacks of FRIA under Art. 27……... 30

2.1.1 The Legal Character and Content Requirements…….. 30

2.1.2 The Temporal Dimension……. 31

2.1.3 The Critical Scope Limitation…….. 33

2.1.4 The Template Questionnaire and MSA Notification…… 33

2.1.5 Sub-Conclusion 1……..... 35

2.2 Deployers and Providers: Roles, Obligations, and Structural Tensions…… 36

2.2.1 The Provider-Deployer Division: Obligations and Their Limits…… 36

2.2.2 The Reliance Mechanism and Territorial Scope……. 39

2.2.3 Sub-Conclusion 2……..... 41

2.3 Liability and Enforcement Architecture…… 41

2.4 Market Surveillance Authorities and National Governance…… 45

2.5 FRIA, HRIA, and DPIA Interaction…… 48

2.6 Conclusions of Chapter II……. 54

**CHAPTER III - IMPLEMENTATION OF A FRIA-TYPE OBLIGATION IN UKRAINE**…….. 58

3.1 Ukraine's Legislative Baseline…….. 58

3.2 Comparative Models and Design Options……. 66

3.3 Potential Institutional Architecture……... 77

3.4. Conclusions of Chapter III……... 79

**CONCLUSIONS**…… 81

**RECOMMENDATIONS**…….. 84

**LIST OF BIBLIOGRAPHY**……. 86

**ABSTRACT**……... 97

**SUMMARY**…… 98

**HONESTY DECLARATIONS**……. 101

# INTRODUCTION

The research problem of this thesis is whether the Fundamental Rights Impact Assessment under Article 27 of the EU AI Act constitutes a genuine *ex ante* fundamental rights protection instrument or whether its internal-market legal basis structurally predetermines it to function as a formalistic compliance mechanism.

*Ex ante* impact assessment of the governance of artificial intelligence represents a change in regulatory logic: instead of a prescriptive rule-setting that reacts to harm in response to it, a preemptive and risk-based regulation aims to spot and address the adverse impacts of a technology before the latter attains the field of application.[1] This change exemplifies a larger phenomenon in EU regulatory law of procedurally incorporating protection of rights into designing and implementing potentially harmful systems, as opposed to just employing *ex post* liability.[2]

The Fundamental Rights Impact Assessment (FRIA) enshrined in Article 27 of Regulation (EU) 2024/1689 (the EU AI Act) represents the most important legal example of this approach to governing algorithms to date. Article 27 requires a specified group of high-risk AI systems deployers - bodies with public law obligations, privately operated organizations offering public service, and those assisting with creditworthiness evaluation and insurance risk assessment, to conduct a FRIA before placing covered systems into operation.[3] At the face of it, such an obligation can be seen as an attempt to operationalize the provisions of the EU Charter of Fundamental Rights (CFR) in the context of deploying AI and convert the principles of human dignity, non-discrimination, privacy, and the right to justice into a binding pre-deployment process.

Nevertheless, a closer look at the legal framework of the AI Act shows that there is a structural tension in it. The Act is grounded in Article 114 TFEU, the internal-market harmonization provision, and adopts the New Legislative Framework (NLF) model developed to integrate the internal market for goods. The NLF places the manufacturer (here, the AI provider) at the center of the regulatory architecture, imposing the Act's strictest and most

---

[1] Alina Wernick, "Impact Assessment as a Legal Design Pattern - A 'Timeless Way' of Managing Future Risks?" *Digital Society* 3, no. 2 (2024): 2-3.

[2] Reuben Binns, "Data Protection Impact Assessments: A Meta-Regulatory Approach," *International Data Privacy Law* 7, no. 1 (2017): 22.

[3] "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," *Official Journal of the European Union* L, 2024/1689, 12 July 2024, Art. 27(1).

heavily harmonised obligations on providers. Consequently, the general rights protection objective, which is enshrined in Article 1 AI Act, becomes not a primary goal but a limitation of an essentially market-integration instrument.[4]

The FRIA itself was a controversial legislative compromise: the original proposal of the Commission did not include a FRIA obligation, the European Parliament added it with Amendment 413 applying to all high-risk deployers, and the final trialogue text was reduced significantly to exclude important procedural aspects - an explicit mitigation plan, thorough consideration of vulnerability, and a mandatory stakeholder process. This design trajectory structurally predisposes the FRIA to become what the scholarship has characterized as 'box-ticking, bureaucratization and ethics-washing' - a bureaucratic check-box exercise rather than a genuine *ex ante* rights-audit.[5] The risk is compounded by Article 27(5), which compels the AI Office to produce a template questionnaire to ease compliance in a simplified way; yet a questionnaire-based approach is structurally incapable of capturing the contextual, expert-dependent nature that a sound FRIA requires.[6] The absence of explicit administrative penalties for failure to comply with Article 27, which falls entirely outside the penalty schedule of Article 99, removes the last enforcement backstop that might otherwise incentivise substantive over cosmetic compliance.[7]

The researched problem has a second face. Ukraine, granted a EU candidate-country status in June 2022, needs to make choices on whether and how to integrate FRIA-type obligations into its developing AI and data protection framework. Ukraine Draft Law No. 8153 On Personal Data Protection,[8] modelling on the GDPR, was passed in first reading in November 2024. At the same time, the Draft Strategy for AI Development to 2030 was presented at the WINWIN Summit in 2025.[9] This interplay between FRIA-type obligations and this emerging legal landscape an underexplored intersection in the legal literature. For Ukraine, the threat is that the Brussels Side-Effect creates the situation where jurisdiction is transplanting the AI Act's

---

[4] Nathalie A. Smuha, *Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law* (Cambridge: Cambridge University Press, 2024), 267.
[5] Marta Lasek-Markey and Linda Hogan, “Delivering on the Promise of the Fundamental Rights Impact Assessments in the EU AI Act: Intersectionality and Vulnerability,” *European Journal of Law and Technology* 16, no. 2 (2025): 1-23.
[6] Alessandro Mantelero, "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template," *Computer Law & Security Review* 54 (2024): 8-9.
[7] Lasek-Markey and Hogan, Delivering on the Promise, 5.
[8] "Draft Law of Ukraine on Personal Data Protection," Verkhovna Rada of Ukraine, Bill No. 8153, 25 October 2022.
[9] "How Ukraine Will Develop AI Strategy till 2030 - the Draft Was Presented," Ministry of Digital Transformation of Ukraine, accessed April 2026.

product safety architecture wholesale, containing its structural limits with its advantages, which is a tangible legislative design challenge.

The answer on the question of why is it necessary to examine the FRIA now, and why cannot this examination be deferred lies in a narrow operational window: the EU AI Act entered into force on 1 August 2024, the FRIA obligation under Article 27 becomes applicable on 2 August 2026, and at the moment this research is completed neither the AI Office template questionnaire mandated by Article 27(5) nor consolidated EU-level operational guidance on methodologically sound FRIA has been published. This means that the crucial period for the development of the FRIA's operational implementation coincides with the period in which this research is conducted.

The relevance also extends to the global level. The recorded propensity for EU regulatory standards to spread internationally - through the de facto Brussels Effect, whereby multinational companies apply EU standards globally, and the de jure Brussels Effect, whereby third country legislators adopt EU frameworks as templates already made for them - means that the quality of the design of Article 27 will have consequences that extend far beyond the Union's borders.[10] If the FRIA turns into a compliance formality, its spread around the world will export a rights protection deficit at scale - a situation, Almada and Radu describe as a "Pyrrhic victory" for European value promotion.[11]

From the Ukrainian point of view, therefore, the relevance is both legislative and constitutional. The absence of interaction between the data protection reform (Draft Law No. 8153) and the AI governance strategy in Ukraine leaves a gap in legislation, which requires scholarly attention. Ukraine's position as a late adopter has the outsider advantage of being able to take notice of the operational limitations of the EU model and add corrective design features - advantages that will be lost if the legislative momentum leads to mechanical transposition without critical evaluation.

The scholarship on the FRIA under the EU AI Act is rapidly developing but it is still arranged around several thematic threads not yet systematically synthesized. Mantelero's 2024 article in Computer Law & Security Review is the most detailed analysis of the genealogical

---

[10] Anu Bradford, "The Brussels Effect," *Northwestern University Law Review* 107, no. 1 (2012): 3, 7-8; Charlotte Siegmann and Markus Anderljung, *The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market* (Oxford: Centre for the Governance of AI, 2022).

[11] Marco Almada and Anca Radu, "The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy," *German Law Journal* 25, no. 4 (2024): 17-18.

origin of the FRIA in HRIA, its normative structure under Article 27, and the methodical obligations for a model template - identifying the lack of a strong methodology for risk quantification as the “elephant in the room” of the AI Act.[12] Gill-Pedro’s 2025 contribution to the European Journal of Law and Technology develops the teleological critique of Article 27, establishing that the regulatory architecture of the Act has a “strong market bias” and that the FRIA is a minimum-harmonisation obligation where deployer decisions are in the nature of “selling arrangements” under Keck and Mithouard.[1314] Lasek-Markey and Hogan identify three categories of limitation (technical, conceptual, and political) arguing that meaningful FRIAs require an intersectionality lens to capture compounded algorithmic harms.[15] The extraterritorial dimension is addressed by Bradford's foundational Brussels Effect theory[16], applied to AI by Siegmann and Anderljung[17], and critically examined by Almada and Radu through the "Brussels Side-Effect" concept.[18]

The wider theoretical picture is provided by Wernick's characterisation of impact assessments as a "legal design pattern",[19] Binns's meta-regulatory analysis of the DPIA,[20] and Götzmann's HRIA methodology framework.[21] On the Ukrainian side, Hura analyses the specific challenges of adapting Ukrainian legislation to the AI Act's risk-classification architecture; Perederii examines the Europeanisation of Ukraine's AI legal order and diagnoses its statutory fragmentation; and Yukhymenko provides the most detailed practitioner-oriented mapping of Ukraine's regulatory implementation options to date. Smuha's monograph on how algorithmic regulation in the public sector erodes rule-of-law values provides the structural theoretical foundation for the critique of Article 27's public-sector deployer scope that runs throughout the thesis.[22] The comparative design literature on the Dutch Fundamental Rights

---

[12] Mantelero, The FRIA in the AI Act, 8.
[13] Eduardo Gill-Pedro, "Fundamental Rights Impact Assessments in the EU's AI Act: A Teleological and Contextual Analysis of the Obligations of Deployers," *European Journal of Law and Technology* 16, no. 3 (2025): 10-16.
[14] Joined Cases C-267/91 and C-268/91, *Criminal Proceedings against Keck and Mithouard,* ECLI:EU:C:1993:905, judgment of 24 November 1993.
[15] Lasek-Markey and Hogan, Delivering on the Promise, 13-21.
[16] Bradford, The Brussels Effect, 1.
[17] Siegmann and Anderljung, The Brussels Effect and Artificial Intelligence, 18.
[18] Almada and Radu, The Brussels Side-Effect, 1-2.
[19] Wernick, Impact Assessment as a Legal Design Pattern, 4-9.
[20] Binns, Data Protection Impact Assessments, 22-23.
[21] Nora Götzmann, "Introduction to the Handbook on Human Rights Impact Assessment: Principles, Methods and Approaches," in *Handbook on Human Rights Impact Assessment*, ed. Nora Götzmann (Cheltenham: Edward Elgar Publishing, 2019), 2-30.
[22] Maksym Hura, "Adaptation of Ukrainian Legislation to the Norms of the EU Artificial Intelligence Act: Challenges and Prospects," *The Journal of V. N. Karazin Kharkiv National University,* Series "Law" 40 (2025): 119-128 [in Ukrainian]; Oleksandr Perederii, "Legal Principles of the Use of Artificial Intelligence in Ukraine in

and Algorithm Impact Assessment (FRAIA), the Canadian Directive on Automated Decision-Making, and Directive (EU) 2024/1760 (CSDDD) supplies the institutional and methodological templates against which Article 27 is measured in Chapter III.[23]

The contribution of this thesis is application-oriented rather than theory-generating. The structural critiques on which the analysis builds (the methodological vacuum and product-safety mismatch identified by Mantelero, the market-bias and minimum-harmonisation diagnosis advanced by Gill-Pedro, and the technical, conceptual and political limitations together with the intersectionality and empowerment requirement formulated by Lasek-Markey and Hogan) already exist in the scholarship. What this thesis adds is threefold. First, it consolidates these existing critiques into a single diagnostic framework usable by Ukrainian legislators, and tests Article 27 against the four-criterion HRIA standard developed by Götzmann together with the empowerment criterion of Lasek-Markey and Hogan, in a unified comparative matrix that also includes the DPIA under Article 35 GDPR. Second, it reads the result of that test through the constitutional architecture of Article 114 TFEU and Article 51(2) of the Charter, in order to distinguish those weaknesses that follow from the legal basis from those that follow from the regulatory model chosen for it - a distinction that matters for the design choices a legislator outside the EU's internal-market framework is free to make. Third, and as the principal original contribution, it translates that diagnosis, together with comparative lessons drawn from the Dutch FRAIA, the Canadian Directive on Automated Decision-Making, and the CSDDD, into a set of legislative design options calibrated to the Ukrainian Constitution, to Draft Law No. 8153 and the National AI Concept, and to Ukraine's wartime institutional capacity. The Ukrainian application is therefore the original layer of the thesis; the EU-side analysis synthesizes and applies the existing literature rather than developing a new theoretical taxonomy.

The theoretical significance is that it contributes to the literature on impact assessment as a human rights methodology in algorithmic governance, in combining the insights of the

---

the Context of the Europeanization of the National Legal System," *The Journal of V. N. Karazin Kharkiv National University*, Series "Law" 40 (2025): 55-61 [in Ukrainian]; Stanislav Yukhymenko, "Analytical Note: AI Regulation - EU Experience and Future Regulation in Ukraine", *Institute for Economic Research and Policy Consulting* (2025), 1-18 [in Ukrainian]; Smuha, Algorithmic Rule By Law, 267.

[23] Janneke Gerards, Mirko Tobias Schäfer, Iris Muis, and Arthur Vankan, Fundamental Rights and Algorithms Impact Assessment (FRAIA) (The Hague: Ministry of the Interior and Kingdom Relations, 2022); "Directive on Automated Decision-Making," Treasury Board of Canada Secretariat, 2019, amended 2025; "Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859," *Official Journal of the European Union* L, 5 July 2024, Arts. 5, 13.

work of Mantelero, Gill-Pedro, Lasek-Markey and Hogan, and the Brussels Effect literature in a single analytical framework going forward to improve understanding of the ways in which fundamental rights obligations can be operationalized in a regulatory architecture oriented towards internal market objectives.

The practical significance of the thesis operates on two levels. For EU deployers subject to Article 27 from 2 August 2026, it identifies the structural deficiencies of the FRIA obligation and derives from that analysis the substantive requirements that a methodologically sound assessment must satisfy. For Ukrainian legislators engaged in finalizing Draft Law No. 8153 and the AI Development Strategy to 2030, it offers a comparative analysis of three proven regulatory models and seven concrete legislative design options calibrated to Ukraine's constitutional framework and institutional capacity.

The institutional significance goes to national DPAs, market surveillance authorities that are designated under Article 70 AI Act, Lithuanian and Ukrainian policymakers, and civil society organizations working on algorithmic accountability advocacy.

This thesis is an original work of personal intellectual, creative, and scientific activity. It has not been previously submitted or defended at Mykolas Romeris University, Taras Shevchenko National University of Kyiv, or any other educational institution in Lithuania, Ukraine, or abroad. The analytical work represents the author's own independent contribution. All sources of other authors are cited in accordance with the requirements of research ethics, and no part of the thesis has been produced through involvement of third persons in the writing process.

The aim of this thesis is to determine whether the Fundamental Rights Impact Assessment under Article 27 of the EU AI Act functions as a genuine *ex ante* human rights protection instrument or as a formalistic compliance mechanism, and to derive from that determination concrete normative design proposals for Ukraine's developing AI and data protection framework.

The objectives of the research are following:

1. To establish the normative criteria against which the FRIA under Article 27 must be assessed, by mapping the constitutional basis of the AI Act, the fundamental rights at stake under the Charter, and the methodological standards of the impact assessment tradition (Chapter I);
2. To diagnose the structural weaknesses of Article 27 FRIA through doctrinal analysis

and systematic comparison with the HRIA and the DPIA (Chapter II); and

3. To formulate, on the basis of that diagnosis and comparative analysis of the Dutch FRAIA, the Canadian Directive on Automated Decision-Making, and the CSDDD, a set of legislative design options for a FRIA-type obligation calibrated to Ukraine's constitutional framework, Draft Law No. 8153, and wartime institutional capacity (Chapter III).

The thesis employs a pluralistic legal methodology. Doctrinal analysis of Article 27 and its related provisions forms the analytical backbone. Comparative analysis, applied to the FRIA alongside the DPIA under Article 35 GDPR and three external regulatory models (the Dutch FRAIA, the Canadian Directive on Automated Decision-Making, and the CSDDD), generates the normative benchmarks against which Article 27 is assessed. Teleological interpretation is used where the statutory text and the instrument's stated fundamental-rights purpose diverge. The normative-prescriptive method converts the comparative findings into specific legislative design options for Ukraine, calibrated to the Constitution of Ukraine, Draft Law No. 8153, the National AI Concept, and the White Paper on AI Regulation.

The thesis comprises three substantive chapters followed by Conclusions and Recommendations.

**Chapter I** establishes the conceptual and normative foundations of the analysis through four thematic sections. Section 1.1 traces the legislative evolution of the AI Act and establishes its Article 114 TFEU basis and New Legislative Framework architecture. Section 1.2 maps the relationship between high-risk AI systems and the Charter of Fundamental Rights, establishing the context-dependent nature of the rights at stake. Section 1.3 analyses the Brussels Effect as the mechanism through which EU regulatory choices propagate globally and distinguishes market-driven convergence from the normatively mandated approximation imposed on Ukraine by its EU candidate status. Section 1.4 develops the genealogy of impact assessment as a human rights methodology, from environmental and social impact assessment through DPIA to HRIA, establishing the normative criteria against which Article 27 is assessed in the subsequent chapters. Section 1.5 draws out the combined implications of these four foundations for the analysis in Chapters II and III.

**Chapter II** constitutes the doctrinal core. Section 2.1 analyses Article 27's legal character, temporal dimension, scope limitations, template-questionnaire architecture, and MSA notification mechanism. Section 2.2 examines the provider-deployer division of

obligations, the reliance mechanism of Article 27(2), and the territorial scope of the FRIA. Section 2.3 analyses the liability and enforcement architecture, including the absence of Article 27 from the penalty schedule of Article 99. Section 2.4 examines the role of market surveillance authorities. Section 2.5 situates the FRIA in relation to the Human Rights Impact Assessment and the Data Protection Impact Assessment through a structured process-and-content comparative matrix. Section 2.6 synthesizes the chapter into a seven-point diagnostic taxonomy, systematizing the converging structural critiques identified in Sections 2.1 through 2.5, which serves as the analytical bridge to Chapter III.

**Chapter III** turns to the forward-looking normative proposal. Section 3.1 maps Ukraine's legislative baseline and identifies the legislative window currently open to Ukraine as an EU candidate. Section 3.2 conducts a comparative analysis of three alternative models and, on that comparative basis together with Ukrainian constitutional and policy sources, develops seven design options for a Ukrainian FRIA mechanism each mapped to one or more of the seven weaknesses diagnosed in Chapter II. Section 3.3 proposes an institutional architecture anchored in a hybrid supervisory model with a staged implementation plan calibrated to Ukraine's wartime institutional capacity. Section 3.4 concludes that the seven options form an interdependent architectural system, not a menu of independent enhancements.

Defense Statements of the research are:

1. The structural position of the FRIA within the EU AI Act's regulatory architecture prevents it from operating as a genuine *ex ante* fundamental rights protection instrument under the CFR. Because the Act is grounded in Article 114 TFEU and built on the New Legislative Framework, its most demanding and uniformly binding obligations fall on providers, who are positioned as the central compliance actors; the deployer, who alone bears the Article 27 FRIA duty, faces an obligation whose procedural floor is low, whose substantive standard is undefined, and whose breach carries no penalty under Article 99(4) - making the FRIA the least enforceable element of the entire regulatory scheme.
2. The danger that the FRIA will become a check-box exercise is not incidental but is structurally embedded in the design choices of Articles 27(3), 27(5) and 99 - choices that, taken together, produce the seven mutually reinforcing structural weaknesses identified in Chapter II.
3. Ukraine's implementation of FRIA-type obligations should not be a mechanical

transplantation of Article 27 but instead should consider crafting a contextually enriched obligation based on HRIA methodology, intersectionality frameworks and on the GDPR DPIA model - with the advantage of learning from the shortcomings of the EU model before enactment.

Declaration on the Use of Artificial Intelligence and Authorial Responsibility.

Artificial-intelligence tools were used in a strictly auxiliary capacity during the preparation of this thesis. Their use was confined to three technical functions: general literature search and identification of potentially relevant academic and regulatory sources, formatting of the text and bibliographic references in compliance with the Mykolas Romeris University requirements and the Chicago Manual of Style (16th edition), and translation of selected Ukrainian-language sources into English.

No artificial-intelligence tool was used to generate, structure, or evaluate the doctrinal, comparative, or normative analysis presented in the thesis. The selection and analysis of legal sources, the interpretation of Article 27 of the EU AI Act and the related Charter, Treaty, and Ukrainian constitutional materials, the construction of the seven-point diagnostic taxonomy in Chapter II, the comparative architecture in Chapter III, and the conclusions and recommendations addressed to Ukrainian legislators were developed independently by the author, who assumes full responsibility for the accuracy of citations, the interpretation of legal materials, and the analytical positions advanced.

## LIST OF ABREVIATIONS

1. **AI** - Artificial Intelligence;
2. **AI Act** - Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence;
3. **CFR / CFREU** - Charter of Fundamental Rights of the European Union;
4. **CoE** - Council of Europe;
5. **DPIA** - Data Protection Impact Assessment;
6. **ECHR** - European Convention on Human Rights;
7. **EU** - European Union;
8. **FRIA** - Fundamental Rights Impact Assessment;
9. **GDPR** - General Data Protection Regulation (Regulation (EU) 2016/679);
10. **HRIA** - Human Rights Impact Assessment;
11. **MSA** - Market Surveillance Authority;
12. **NLF** - New Legislative Framework;
13. **TEU** - Treaty on European Union;
14. **TFEU** - Treaty on the Functioning of the European Union.

# CHAPTER I

# CONCEPTUAL AND NORMATIVE FRAMEWORK

The chapter establishes the conceptual and normative foundations on which the analysis of the Fundamental Rights Impact Assessment under the AI Act proceeds. Section 1.1 traces the legislative history of the AI Act with emphasis on its internal-market constitutional basis under Article 114 TFEU and the New Legislative Framework model, demonstrating that the structural characteristics of the FRIA are consequences of the instrument's legal architecture rather than choices of legislative drafting. Section 1.2 maps the range of Charter rights engaged by high-risk AI systems and their inherent context-dependency, establishing the substantive standard against which the scope of Article 27 is measured in Chapter II. Section 1.3 examines the Brussels Effect as the mechanism by which EU regulatory choices acquire global significance, distinguishing the voluntary market-driven convergence it typically produces from the legally obligated approximation that Ukraine's EU candidate status entails and which frames the analysis of Chapter III. Section 1.4 surveys the human rights impact assessment tradition (from the GDPR's DPIA through the methodology frameworks of Mantelero and Götzmann) deriving the normative criteria that a genuine FRIA must satisfy.

## 1.1 Legislative Development of the EU AI Act and the FRIA Obligation

To analyze the Fundamental Rights Impact Assessment within the AI Act, it is necessary to first outline the legislative process that resulted in creation of the regulatory framework within which this tool functions. The AI Act represents the current apex of a long history of regulatory progress in the European Union. It is the resultant stage of a decade-long process during which the European Union had worked out a more and more comprehensive approach to the regulation of the digital economy due to the dual purpose of promotion of innovation and safeguarding fundamental rights. The regulatory genealogy starts with the General Data Protection Regulation, which was adopted in 2016, became applicable from 25 May 2018 and formed the main principle according to which the processing of personal data should not violate basic rights and freedoms, in particular, the right to the protection of personal data.[24] The GDPR established a risk-based model of regulation that, while structurally distinct

[24] "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, and Repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union* L

from the AI Act's regulatory approach, shares the same 'risk-based' label and operates in parallel within the EU's broader digital regulatory ecosystem.[25] In February 2020, the European Commission released the White Paper on Artificial Intelligence[26] - A European Approach to Excellence and Trust, which made the regulatory issue a question of economic competitiveness versus fundamental rights and safety. In April 2021, the Commission presented a formal legislative proposal[27], which outlined a risk-based regulatory framework of AI systems.

The legislative history of the FRIA in this process is most informative. There was no mention of a mandatory fundamental rights impact assessment in the original proposal of the Commission. The FRIA was an amendment that came during deliberation of the proposal by the European Parliament, which was seen as a realization that the risk-based approach needed a deployment-stage assessment mechanism of fundamental rights impact. However, the trilogue negotiation between the Parliament, the Council, and the Commission, as Mantelero has recorded, reduced the FRIA obligation considerably: the compromise version contained a much narrower obligation, which most crucially was substantially narrowed to a subset of deployers (primarily public law bodies and private entities delivering public services) with the broad Parliament amendment applying to all high-risk deployers abandoned.[28] The amended version of Article 27 that restricts the FRIA to deployers who are either public law bodies or private entities delivering public services is a form of political trade-off as opposed to a fundamental exposition of the correct scope of the FRIA. This legislative history plays a crucial role in assessing the design of the FRIA because it demonstrates that the tool was created and limited by institutional dynamics.

This legislative trajectory cannot be fully understood without examining its constitutional foundation: the legal basis on which the AI Act rests determines what the instrument is constitutionally capable of achieving.

Article 114 of the Treaty on the Functioning of the European Union, which provides the primary legal basis for the AI Act, is of constitutional significance to the FRIA and must be

---

119, 4 May 2016, Recital 1-2.

[25] Raphaël Gellert, "The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?," *Journal of Ethics and Legal Technologies* 3, no. 2 (2021): 17-20, 27.

[26] "White Paper on Artificial Intelligence - A European Approach to Excellence and Trust," European Commission, COM(2020) 65 final, Brussels, 19 February 2020.

[27] "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," European Commission, COM(2021) 206 final, Brussels, 21 April 2021.

[28] Mantelero, The FRIA in the AI Act, 7-8.

examined closely.[29] Article 114 confers on the Union the competence to approximate Member State legislation relating to the establishment and operation of the internal market, which means that the AI Act is, in its constitutional identity, an internal market harmonisation instrument and not a fundamental rights statute.[30] That is, it aims to eliminate barriers to trade in AI systems by establishing equal rules across Member States. Almada and Radu observe that the Act attempts to accommodate the protection of fundamental rights within this internal-market structure - a structural accommodation that, as will be shown, carries concrete consequences for the design and effectiveness of the FRIA.[31]

This observation requires qualification, and the qualification is itself analytically important. Scholarship on Article 114 TFEU has demonstrated that the provision has evolved well beyond its original function as a deregulatory instrument. The creation of the internal market is no longer conceived as the mere removal of trade barriers but as the construction of a common regulated market in which market integration and the protection of social, environmental, and rights-based interests operate together. The GDPR itself (the direct regulatory precursor to the AI Act) was adopted on the basis of Article 114 TFEU and has produced, by general consensus, a regulatory framework capable of generating substantive fundamental rights protection. The constitutional obligation to observe the Charter of Fundamental Rights when exercising internal market competence (Article 51(1) CFR) reinforces the conclusion that market-building and rights protection are not structurally exclusive categories.[32]

The structural problem identified in this thesis is therefore not a claim that Article 114 TFEU is inherently incompatible with rights protection. It is a more specific and more analytically precise: that the specific regulatory model through which the AI Act implements its Article 114 competence (the New Legislative Framework product safety architecture) is structurally ill-suited to the rights-assessment function that the FRIA is meant to perform. As Almada and Petit have established, the choice to pattern the AI Act on product safety regulation is not a constitutional requirement of Article 114 - it is a legislative choice. The Digital Services Act and the Digital Markets Act rest on the same legal basis but adopt neither the NLF

[29] AI Act, Recital 3.
[30] "Treaty on the Functioning of the European Union (Consolidated Version)," *Official Journal of the European Union* C 326, 26 October 2012, Art. 114.
[31] Almada and Radu, The Brussels Side-Effect, 3.
[32] Charter of Fundamental Rights of the European Union, *Official Journal of the European Union* C 326, 26 October 2012, Art. 51(1); Gellert, "The Role of the Risk-Based Approach," 17, 27.

conformity assessment logic nor the pre-classified risk architecture of the AI Act.[33] The structural problem originates not in the legal basis but in what the legislator built upon it.

That choice has two concrete consequences that bear directly on the FRIA. First, under Article 51(2) CFR, the Charter does not extend the competences of the Union, and the EU possesses no stand-alone competence to legislate on fundamental rights as an independent legislative objective.[34] Rights protection in the AI Act therefore functions as a constraint on the exercise of internal market competence - not as its primary aim. The textual evidence is in the Act itself: Recital 1 establishes that the purpose of this Regulation is to improve the functioning of the internal market, with rights protection listed as a secondary consideration.[35] Second, the risk-based methodology that the NLF model requires is structurally incompatible with the logic of fundamental rights. A risk-based framework assesses impacts on a graduated scale, permits individual harms to be weighed against aggregate societal benefits, and is oriented toward probabilistic harm at a population level. Fundamental rights, as Ebers explains following Yeung and Bygrave, do not operate on a sliding scale: an activity that violates a fundamental right is either lawful or unlawful - the degree of harm does not convert a rights violation into an acceptable risk.[36] The FRIA, placed within a product-safety risk architecture, is thus asked to perform a rights-legality assessment using instruments designed for risk optimization. The Act follows the New Legislative Framework's provider/deployer division, examined in Section 2.2.

This product-safety architecture carries inherent limitations when applied to fundamental rights protection. Almada and Radu argue that the approach is structurally prone to failure because the logic of product safety pertains to physical products, whereas the rights effects of socio-technical AI systems are context-dependent and resist standardized assessment.[37] Gill-Pedro reinforces this critique through a teleological analysis: the NLF model, designed for the safety of machinery and electrical equipment, is ill-suited to fundamental rights obligations that must be context-specific and use-phase-dependent, requiring assessment by the entity actually deploying the system into a given social context.[38]

---

[33] Marco Almada and Nicolas Petit, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?* EUI RSC Working Paper 2023/59 (Florence: European University Institute, 2023), 12.
[34] Charter of Fundamental Rights of the European Union, Art. 51(2); Almada and Petit, "The EU AI Act".
[35] AI Act, Recital 1.
[36] Martin Ebers, "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act," *European Journal of Risk Regulation* 16, no. 2 (2025): 7, citing Karen Yeung and Lee A. Bygrave, "Demystifying the Modernised European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship," *Law, Innovation and Technology* 14 (2022): 201.
[37] Almada and Radu, The Brussels Side-Effect, 7.
[38] Gill-Pedro, Fundamental Rights Impact Assessments, 10-14.

De Cooman demonstrates that the AI Act's NLF-derived scope classification leaves demonstrably high-risk systems outside the regulatory perimeter.[39] The insufficiency of this framework is compounded, by the reliance on conformity assessments that are largely provider self-assessments - a mechanism that raises serious questions about the adequacy of fundamental rights protection.[40]

Building on this product-safety mismatch, the FRIA's scope problem is compounded by the classification logic underlying its trigger: its activation depends on Annex III classification, meaning the arbitrariness of the classification is inherited by the obligation itself. Article 5 forbids the use of AI that creates unacceptable risks, such as the practice of social evaluation by the state, remote biometric identification in the presence of other people (with some exceptions), and capitalizing on the vulnerabilities of certain groups.[41] Articles 6-51, when incorporated together with Annex III, create the regulatory framework of high-risk AI systems, requiring risk management, data governance, transparency, human oversight, accuracy, robustness, and cybersecurity.[42] AI systems with limited risk have transparency requirements, whereas minimal-risk systems have no requirements.[43] Ebers has suggested that, although a risk-based regulation is indeed the correct way to regulate AI, significant provisions in the AI Act are not risk-based, but rather a product of a political trade-off at a given moment in time, and as such, is mostly arbitrary.[44] Gellert's comparative analysis demonstrates that the AI Act's risk-based approach is a structurally narrower regulatory model than the GDPR's: rather than using risk as a compliance tool, it deploys risk solely to determine which AI systems fall within the regulatory perimeter - a design choice that limits its scope to pre-classified high-risk systems and renders its risk thresholds susceptible to the regulator's risk appetite and Type I/II classification errors.[45]

The AI Act is not a standalone instrument but a component of a larger EU digital regulatory ecosystem. Its Recitals directly recognize its interaction with the GDPR, the Data Governance Act, and the Digital Services Act.[46] This creates a complicated compliance

---

[39] Jérôme De Cooman, "Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act," *Market and Competition Law Review* 6, no. 1 (2022): 49-90.
[40] Oskar J. Gstrein, "European AI Regulation: Brussels Effect versus Human Dignity?" *Zeitschrift für Europarechtliche Studien* 25, no. 4 (2022): 12-15.
[41] AI Act, Art. 5.
[42] AI Act, Arts. 6-51; Annex III.
[43] AI Act, Arts. 50, 95.
[44] Ebers, "Truly Risk-Based Regulation," 9.
[45] Gellert, "The Role of the Risk-Based Approach," 15-33.
[46] AI Act, Recitals 1-11.

environment in which deployers of high-risk AI systems may simultaneously be subject to a DPIA under GDPR Article 35, a FRIA under AI Act Article 27, and further obligations under the Digital Services Act or sector-specific legislation. The resulting double regulatory burdens have been documented by Ebers, who notes that the AI Act operates alongside the GDPR, the Medical Devices Regulation, and the Machinery Regulation, imposing overlapping and at times conflicting obligations that raise compliance costs.[47] While Article 27(4) of the AI Act permits the FRIA to be performed in conjunction with the DPIA, the two instruments differ in their scope, their rights benchmarks, and their procedural requirements, so that real integration is more complicated than the legislative text implies.[48] This constitutes what De Vries, Kanevskaia, and de Jager term 'Internal Market 3.0' - a new generation of EU regulation that applies market-integration logic to the digital realm whose overlapping instruments lack the coherence required for systemic rights protection, meaning that Article 27 does not operate in isolation: its effectiveness depends on how it interacts with the DPIA, the DSA's systemic risk assessment obligations, and sector-specific impact assessment requirements - an interaction that the AI Act does not clearly resolve.[49]

Overall, the regulatory design of the AI Act is a combination of institutional decisions that are made in layers. Its legal basis under Article 114 TFEU makes the protection of rights secondary to the rationality of market-integration; the NLF architecture imposes product safety logic on systems, the rights effects of which are inherently context-dependent; and even the FRIA became more of a manifestation of political bargain rather than rights protection tool.

### 1.2 Fundamental Rights in EU Law and Their Engagement with High-Risk Artificial Intelligence

Section 1.2 maps three analytical foundations required for the argument developed in Chapter II: first, the constitutional basis on which fundamental rights protection operates within EU law and the structural implications of that basis for the FRIA's personal scope; second, the range of Charter rights most directly engaged by high-risk AI deployment; and third, the limits of the pre-existing EU legal instruments in addressing AI-related fundamental rights risks, and the systematic assessment gap that Article 27 FRIA was designed to fill.

The constitutional foundation of fundamental rights protection within the EU's AI

[47] Ebers, Truly Risk-Based Regulation, 13-14.
[48] Mantelero, The FRIA in the AI Act, 5-6.
[49] Sybe de Vries, Olia Kanevskaia, and Rik de Jager, "Internal Market 3.0: The Old 'New Approach' for Harmonising AI Regulation," *European Papers* 8, no. 2 (2023): 590-592, 602-603.

regulatory framework is established by Articles 2 and 6 of the Treaty on European Union, which respectively designate respect for human rights as a foundational value of the Union and grant the Charter of Fundamental Rights the same legal status as the Treaties, making it primary EU law.[50] However, the scope of Charter application is governed by a structural constraint of first importance. Article 51(1) CFREU confines the Charter's addressees to EU institutions and to Member States 'only when they are implementing Union law'; Article 51(2) expressly provides that the Charter shall not extend the field of application of Union law beyond the powers of the Union, nor establish any new power or task.[51] The EU possesses no stand-alone competence to legislate on fundamental rights as such: the protection of fundamental rights operates as a side constraint on the exercise of competences conferred by the Member States, rather than as an independent aim of Union action. The AI Act was adopted on the basis of Article 114 TFEU, and as Almada and Petit demonstrate, its primary aim is to facilitate the free movement of AI technologies within the internal market, with fundamental rights protection functioning as a limiting condition rather than a foundational mandate.[52]

Article 51(1) CFREU confines the Charter's addressees to EU institutions and to Member States only when implementing Union law; it does not extend to private parties, and the Charter produces no general horizontal direct effect in private legal relations. The FRIA's restricted personal scope under Article 27 is a direct consequence of this constitutional ceiling: private commercial deployers are excluded not because their deployments present lesser rights risks, but because the Article 114 TFEU basis does not support a general fundamental rights obligation absent a public-service nexus, a constraint examined in detail in Chapter II.[53] Its extension to private conduct can occur only indirectly, where secondary Union law independently imposes obligations on private actors - a design feature that limits its relevance for AI deployers who are not public law bodies or entities performing public functions. Muir has shown that the resulting case-by-case expansion produces an apparent widening of horizontal Charter application that is in practice determined by the accidents of litigation rather than by any principled account of the circumstances in which private actors bear fundamental

[50] Treaty on European Union (Consolidated Version), *Official Journal of the European Union* C 326, 26 October 2012, Arts. 2, 6.
[51] Charter of Fundamental Rights of the European Union, Art. 5(1)-(2).
[52] Almada and Petit, The EU AI Act, 9-12; Ebers, Truly Risk-Based Regulation, 7; Commission Proposal COM(2021) 206 final, Annex I.
[53] Koen Lenaerts, "Exploring the Limits of the EU Charter of Fundamental Rights," *European Constitutional Law Review* 8, no. 3 (2012), 376-377.

rights duties.[54] Spaventa demonstrates that Article 51(2) was inserted precisely to address Member States' fears of competence creep, and that the Court has adopted a correspondingly narrow interpretive approach - one that Spaventa herself critiques as unduly restrictive.[55]

The Court of Justice has nonetheless progressively extended Charter obligations to private actors in specific, right-by-right contexts. In Google Spain, the Court interpreted the right to be forgotten (grounded in the informational self-determination interests protected by Articles 7 and 8 CFREU) against the background of the EU Data Protection Directive, imposing a Charter-aligned obligation on Google as a private operator.[56] In Egenberger, the Court went further and recognised the horizontal direct effect of the right to non-discrimination under Article 21 CFREU in an employment relationship between private parties.[57] Yet, as Muir observes, this progression remains right-by-right and case-by-case: it does not constitute a systematic doctrine.[58] Lasek-Markey and Hogan confirm that to date only Articles 21, 31(2), and 47 CFREU have been declared by the Court capable of direct horizontal effect; the broader Charter rights most relevant to high-risk AI deployment (including dignity, child rights, worker protection, and social security) have not been given such effect absent implementing secondary legislation.[5960] This doctrinal uncertainty bears directly on the FRIA. The FRIA obligation under Article 27 is limited to bodies governed by public law and private entities delivering public services - a restriction that reflects not a rights-risk judgment but the constitutional ceiling imposed by Article 51(2) CFREU and Article 114 TFEU: a general FRIA mandate extending to all private deployers would require the EU to legislate beyond the limits of its internal market competence - a constitutional ceiling that, as established above, Article 114 TFEU and Article 51(2) CFR together impose on any internal-market instrument that seeks to pursue fundamental rights protection as an independent objective.[61] A private commercial deployer of an identical system falls outside Article 27 not because its deployment presents a lesser risk to fundamental rights, but because the internal market legal basis does not support a

---

[54] Elise Muir, "Fundamental Rights: An Unsettling EU Competence," *Human Rights Review* 15, no. 1 (2014): 30-32.
[55] Eleanor Spaventa, The Interpretation of Article 51 of the EU Charter of Fundamental Rights: The Dilemma of Stricter or Broader Application of the Charter to National Measures, *European Parliament Policy Department C Study*, PE 556.930: 5-6.
[56] Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos, ECLI:EU:C:2014:317.
[57] Case C-414/16, Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV, ECLI:EU:C:2018:257.
[58] Muir, Fundamental Rights: An Unsettling EU Competence, 30-32.
[59] Lasek-Markey, and Hogan, Delivering on the Promise, sections 5-6.
[60] Case C-176/12, Association de médiation sociale v. Union locale des syndicats CGT, ECLI:EU:C:2014:2, judgment of 15 January 2014, §§45-49.
[61] Article 51(2) CFREU; Almada and Petit, EUI RSC Working Paper 2023/59, 12, 17-18.

general fundamental rights obligation in the absence of the public-service nexus. The structural implications of this limitation are examined in Chapter II.

### 1.3 The "Brussels Effect" and the Global Stakes of FRIA Design

Before the structural weaknesses of the Fundamental Rights Impact Assessment under Article 27 of the AI Act are examined in Chapter II, it is necessary to establish why the quality of that design carries consequences extending well beyond the European Union. The answer lies in the Brussels Effect - the mechanism through which EU regulatory standards propagate internationally and shape the governance choices of multinational companies and third-country legislators alike. If the FRIA model embedded in Article 27 becomes a global regulatory reference point, the structural deficiencies that this thesis identifies will not remain confined to EU deployers: they will travel. Establishing the scope, the limits, and the critical conditions of that diffusion is therefore necessary before undertaking the FRIA analysis, and equally serves to situate the analysis within its Ukrainian context.

The Brussels Effect, introduced by Anu Bradford in her 2012 article published in the Northwestern University Law Review, refers to the process by which the European Union imposes its regulatory principles globally by exercising its market power.[62] Bradford identifies five conditions that enable this mechanism: market size (the EU single market offers a consumer base sufficiently large that global companies cannot afford to ignore it); regulatory capacity (the EU possesses the institutional presence to design and enforce complex regulation); preference for stringent regulation (the EU consistently sets higher standards than competing regulatory regimes in areas of consumer, environmental, and rights protection); the targeting of inelastic targets (regulation applies to activities that cannot easily be relocated to other jurisdictions); and non-divisibility of standards (maintaining a single global compliance standard is more cost-effective than operating separate compliance frameworks in different markets).[63] These conditions generate two complementary dynamics: the de facto effect, where firms voluntarily apply EU standards globally, and the de jure effect, where third-country legislators adopt EU regulatory frameworks as legislative templates. The paradigm case in the digital domain is EU privacy regulation: Bradford demonstrates that EU data protection rules prompted more than thirty countries to adopt comparable frameworks following the 1995 Data Protection Directive,[64] and Siegmann and Anderljung confirm that the GDPR has since served

[62] Bradford, The Brussels Effect, 1, 10-18.
[63] Ibid., 10-18.
[64] Ibid., 22-25.

as a legislative model for jurisdictions including California, Virginia, and China, while multinational companies have adopted a single EU-compliant data governance standard globally rather than maintaining separate compliance frameworks in different markets.[65]

Siegmann and Anderljung have applied Bradford's analytical framework directly to the AI Act and argue that several Brussels Effect conditions are satisfied: the size of the EU market gives it leverage over AI developers worldwide, the AI Act regulates inelastic targets (the use of AI systems within EU territory cannot be relocated), and non-divisibility considerations incentivise companies to implement its requirements globally.[66] If these predictions prove accurate, Article 27's FRIA model could emerge as the de facto international benchmark for fundamental rights evaluation of AI systems - a consequence that transforms the quality of Article 27's design from a European regulatory question into a matter of global concern.

This prospect is, however, subject to a significant structural caveat identified in the critical literature. Almada and Radu have developed the concept of the Brussels Side-Effect: rather than spreading EU values globally, the AI Act risks spreading its structural deficiencies.[67] Their central argument rests on the same legal foundation that Section 1.1 of this thesis has established as central to the FRIA analysis - the AI Act is grounded in Article 114 TFEU, the internal-market harmonisation provision, and adopts a product-safety regulatory architecture that is not structurally oriented towards the protection of fundamental rights. The primary purpose of an Article 114 instrument is the opening and functioning of markets, not the guarantee of rights: as Almada and Radu observe, the Act does not target the protection of rights as its main objective, but the opening and shaping of markets.[68] They further establish that the product-safety risk formula is structurally inconsistent with the logic of fundamental rights as a matter of regulatory methodology, not merely of legislative drafting.[69] The Brussels Side-Effect argument thus connects the macro-level question of global regulatory diffusion directly to the micro-level architecture of Article 27: when a rights-assessment mechanism embedded within a market-integration instrument propagates through the Brussels Effect, what travels is the compliance documentation architecture - not the rights-protective substance that a genuine human rights impact assessment methodology would require. This is precisely the structural mismatch that Chapter II diagnoses in detail.

---

[65] Siegmann and Anderljung, The Brussels Effect and Artificial Intelligence, 18-29, Appendix 4.1.
[66] Ibid., 18-29.
[67] Almada and Radu, The Brussels Side-Effect, 1-2.
[68] Ibid., 3.
[69] Ibid., 7.

The distinction between voluntary market-driven convergence and normatively mandated approximation (which characterizes Ukraine's position as an EU candidate state bound by the legal obligations of the Association Agreement of 2014 and the accession process) is examined in Chapter III, where it informs the argument that Ukraine's implementation of FRIA-type obligations should take the form of adaptive rather than mechanical transposition of Article 27's structural architecture.

### 1.4 The Impact Assessment Tradition as a Human Rights Methodology

Impact assessment, in its widest meaning, can be described as a regulatory methodology that aims at predicting and measuring the impacts of proposed activities prior to their implementation. Wernick characterises impact assessments as a pattern of distinct legal design - a reusable, abstract problem-solving model that legislators deploy across a variety of regulatory contexts where it is necessary to determine the future consequences of an activity and to follow the course of action most favourable to the values in question. Wernick grounds her concept in the architectural theory of pattern languages developed by Christopher Alexander, treating the recurring regulatory problem of uncertain future harm as a structural problem amenable to a repeatable solution.[70] This framing is analytically significant for the purposes of this thesis: it allows the FRIA under Article 27 to be read not as an *ad hoc* construction of the AI Act but as a particular instance of an established legal design template, susceptible to the same underlying tensions and design dilemmas that characterise any project-based impact assessment - tensions that, as Chapter II will demonstrate, are reproduced in and intensified by the specific product-safety architecture within which the FRIA is embedded.

Wernick further characterises the obligatory impact assessment as a form of enforced self- or meta-regulation: the regulator mandates the conduct of the assessment while delegating to the regulated entity the task of identifying and evaluating the risks in question, on the assumption that the regulated entity is best placed to understand and manage those risks. There are inherent tensions in this delegation structure identified by Wernick.[71] The FRIA under Article 27 is particularly susceptible to the epistemic and regulatory tensions: deployers are required to assess technically complex AI systems whose design they neither control nor may fully understand, while the self-regulatory structure of the FRIA leaves the evaluation in the hands of the same organization whose operations are under scrutiny. Both vulnerabilities are

[70] Wernick, Impact Assessment as a Legal Design Pattern, 7-8.
[71] Ibid., 11-13, 15-18.

examined in detail in Chapter II.

The closest predecessor of the FRIA in EU law is the Data Protection Impact Assessment under Article 35 of the GDPR.[72] The DPIA mandates that, before processing, data controllers evaluate how the planned processing operations would affect the security of personal information, particularly where processing involves new technologies and is likely to pose a significant threat to the rights and freedoms of natural persons. The DPIA, as Mantelero has noted, builds on a prior history of *ex ante* assessment of processing operations (most notably the Privacy Impact Assessment process that emerged over the course of the 1990s) and shares with the FRIA its circular, iterative design, intended to accompany technological systems throughout their operational lifetime rather than serve as a one-time compliance exercise.[73] Nevertheless, the DPIA is structurally confined to data protection and privacy risks. It does not extend to the full range of Charter rights that AI systems can engage - and it is precisely this gap that the FRIA was designed to fill.

The wider tradition of the Human Rights Impact Assessment provides the normative standard against which the FRIA must be measured. The HRIA tradition in its contemporary form is rooted in the United Nations Guiding Principles on Business and Human Rights, adopted in 2011, which established the foundational tripartite framework: the state duty to protect human rights, the corporate responsibility to respect human rights, and the right of affected persons to access remedy in cases of business-related human rights violations.[74] Mantelero, who has played a central role in translating this tradition to the context of AI governance, proposed in 2018 a blueprint for a human rights, social, and ethical impact assessment of AI and big data technologies, observing that the conventional DPIA was insufficient to capture the broader societal impact of these technologies on fundamental rights.[75] Mantelero explicitly framed this model as a voluntary self-assessment mechanism - a design choice that distinguishes it from the mandatory FRIA obligation subsequently introduced by Article 27 of the AI Act. This was further subsequently developed into a rigorous evidence-based methodology by Mantelero and Esposito, who argue that human rights alone provide a sufficiently universal reference framework for regulating AI across diverse cultural, ethical, and legal contexts, and that ethics-based approaches - as opposed to rights-based approaches -

---

[72] GDPR, Art. 35.
[73] Mantelero, The FRIA in the AI Act, 4.
[74] Guiding Principles on Business and Human Rights, United Nations HR/PUB/11/04 (2011), 1, 3, 13, 27.
[75] Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment,' *CLSR* 34, no. 4 (2018): 754-772.

generate uncertainty, heterogeneity, context-dependence, and the risk of privileging particular community values over universally binding obligations.[76]

Building on this tradition, Götzmann identifies four process criteria that distinguish a genuine HRIA from other types of impact assessment. First, it must be grounded in international human rights standards as the authoritative normative benchmark.[77] Second, it must ensure the effective involvement of rights-holders as active participants in the assessment process, rather than treating them as passive subjects. Third, it must be attentive to equality and non-discrimination, so that aggregate societal benefits do not obscure differential harms to particular groups. Fourth, it must be grounded in accountability - encompassing transparency, access to information throughout the process, the identification of duty-bearers, and enforceable access to remedy for those affected.[78] Together, these four criteria constitute the operational standard of a genuine HRIA - a standard against which Article 27 is measured in full in Chapter II, Section 2.5.

Mantelero's 2024 analysis of the FRIA under the AI Act proposes a three-phase template for a methodologically sound fundamental rights assessment. The first phase concerns planning and scoping: determining whether a FRIA is required, identifying the relevant rights and the potentially affected rights-holders, and defining the assessment's parameters. The second phase is risk analysis: gathering contextual evidence, evaluating the probability and severity of rights impacts, and mapping the differential effects on distinct groups of rights-holders. The third phase addresses risk management: designing and implementing mitigation measures, undertaking re-engineering of the system where necessary, and establishing iterative monitoring mechanisms.[79] Mantelero presents this framework as a continuous and circular process - a sequence of successive assessment loops rather than a single pre-deployment compliance event. This stands in direct contrast to the structure of Article 27, which requires deployers to identify measures to be taken in the event that risks materialise but imposes no obligation to implement those measures, to monitor their effectiveness, or to revisit the assessment as deployment conditions evolve. The three-phase model, read against Article 27, exposes the temporal dimension of the FRIA's structural weakness - a dimension examined further in Chapter II.

---

[76] Alessandro Mantelero and Maria Samantha Esposito, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems,' CLSR 41 (2021): 4-5.
[77] Götzmann, Introduction to the Handbook on HRIA, 6-9.
[78] Ibid., 6-9.
[79] Mantelero, The FRIA in the AI Act, 5-9, 15-17.

Against this normative background, the criteria of a genuine Fundamental Rights Impact Assessment, as established by Götzmann and Mantelero within the HRIA tradition, can be stated as follows: it must be anchored in international human rights standards (in this context the CFREU) as its authoritative frame of reference; it must be participatory, ensuring the meaningful involvement of affected rights-holders as active agents rather than passive subjects; it must be attentive to equality and non-discrimination, so that differential harms to specific groups are not obscured by aggregate findings; it must be grounded in accountability - encompassing transparency, access to information, identification of duty-bearers, and access to remedy for those affected.

The FRIA under Article 27 of the AI Act falls short against each of these criteria. Recital 48 acknowledges that a broad range of Charter rights may be affected by high-risk AI systems, yet the Article 27 procedure does not guarantee the identification of all rights engaged in a specific deployment, the meaningful involvement of affected persons, or any enforceable accountability for the outcome. This shortfall is not incidental: as Sections 1.1 and 1.3 have established, it is structurally embedded in the choice to ground the AI Act in an Article 114 TFEU product-safety architecture - a choice that configures fundamental rights protection as a secondary constraint on market integration rather than as the instrument's primary mandate. The discrepancy between the normative standard established in this section and the procedural design of Article 27 is the central conflict that Chapter II diagnoses systematically.

### 1.5 Conclusions of Chapter I

Chapter I has identified four structural conditions that together determine whether the FRIA under Article 27 can function as a genuine rights-protection instrument or whether it is destined to operate as a formalistic compliance requirement. This concluding section draws out their combined implications for the analysis in Chapters II and III.

The deployment of high-risk AI systems engages a broad range of Charter rights (including human dignity, privacy and data protection, non-discrimination, effective remedy, and social rights) and does so in a manner that is inherently context-dependent: the same system may produce different rights implications depending on how, where, and against whom it is used.[80] This context-dependency is precisely what necessitates a deployment-stage assessment rather than a pre-market technical evaluation alone. Yet the AI Act within which the FRIA sits is constitutionally an internal market harmonization measure grounded in Article 114 TFEU,

[80] FRA, Getting the Future Right, 7-8.

not a fundamental rights instrument.[8182] The New Legislative Framework model places the provider at the center of the regulatory architecture, while the deployer who bears the FRIA obligation faces a procedural floor that, as Gill-Pedro's teleological analysis demonstrates, functions as minimum harmonization - leaving the most stringent and fully harmonized obligations exclusively on the provider side. The FRIA therefore exists within a regulatory architecture that was not designed to carry it.

The global significance of these structural features is mediated through the Brussels Effect, though its operation in the AI context differs materially from the GDPR's pattern of extraterritorial reach.[8384] For Ukraine, the critical distinction is that regulatory convergence arises not from market incentives but from the legal obligations of EU candidate status - a constraint that simultaneously limits design choices and creates the legislative space to address the structural limitations that the EU model carries as a consequence of its market-integration origins. The normative standard against which both models are assessed is derived from the HRIA tradition: a methodologically adequate fundamental rights impact assessment must be grounded in international human rights standards, participatory in its engagement with affected rights-holders, sensitive to differential impacts, transparent and accountable in its methodology, and iterative rather than a one-time pre-deployment formality.[85]

Chapter II asks whether Article 27 satisfies these criteria - or whether, as the constitutional and structural analysis of this chapter suggests, it replicates the form of a rights-assessment tool without its methodological, institutional, or procedural substance. Chapter III then examines whether the structural weaknesses identified in that diagnosis can be addressed through Ukraine's implementing legislation, or whether the requirements of regulatory approximation necessitate their reproduction.[86]

---

[81] Gill-Pedro, Fundamental Rights Impact Assessments, §3.1.1, §3.1.3, §3.2.4.
[82] Smuha, Algorithmic Rule By Law, 267.
[83] Bradford, The Brussels Effect, 3, 7-8.
[84] Almada and Radu, The Brussels Side-Effect, 13-14; Siegmann and Anderljung, The Brussels Effect and Artificial Intelligence, 69.
[85] Götzmann, "Human Rights Impact Assessment of Business Activities," *Business and Human Rights Journal* 2, no. 1 (2017): 92-99.
[86] Gill-Pedro, Fundamental Rights Impact Assessments, §3.3.2.

# CHAPTER II

# FUNDAMENTAL RIGHTS IMPACT ASSESSMENT UNDER AI ACT: THE COMPREHENSIVE ANALYSIS

Chapter I established four structural conditions that predetermine the capacity of the FRIA to function as a genuine rights-protection instrument: the constitutional subordination of rights protection to the internal-market logic of Article 114 TFEU, the context-dependent character of the Charter rights that Article 27 is meant to protect, the mechanism through which the design choices embedded in Article 27 may travel globally through the Brussels Effect, and the normative standard of methodologically adequate rights assessment derived from the HRIA tradition. Chapter II applies those foundations to a question they make it possible to answer: whether Article 27, as enacted, meets the normative standard that Chapter I established, or whether it fulfils the documentary form of rights assessment while lacking the methodological, institutional, and procedural substance that a genuine *ex ante* fundamental rights protection mechanism requires.

Section 2.1 examines Article 27's legal character, temporal structure, personal scope, and template-questionnaire architecture - establishing that each of these design elements produces a discrete structural constraint on the FRIA's rights-protective capacity, and that these constraints are not incidental but are consequences of the legislative choices traced in Chapter I. Section 2.2 analyses the provider-deployer division of obligations and the Article 27(2) reliance mechanism, demonstrating that the structural asymmetry identified in Section 1.1 is reproduced at the operational core of the FRIA and generates the informational dependency weakness. Section 2.3 diagnoses the enforcement architecture, identifying four discrete gaps each of which severs the FRIA from the accountability structure that Götzmann's fourth criterion requires. Section 2.4 examines the institutional architecture of MSA oversight, revealing that the product-safety mandate of the designated supervisory authority, the MSA-DPA jurisdictional bifurcation, and the co-regulatory delegation of standard-setting to commercially-dominated ESOs together compound the enforcement deficit with an institutional misfit. Section 2.5 situates the FRIA comparatively against the HRIA and the DPIA through a six-dimension matrix and a ten-criterion HRIA taxonomy, establishing that Article 27 fails to satisfy any of Götzmann's four process criteria as binding requirements and that the coexistence of overlapping assessment obligations without structural integration generates

assessment fragmentation. Together, these five diagnoses are synthesized in Section 2.6 into a seven-point diagnostic taxonomy that maps the converging structural deficiencies of Article 27 to concrete legislative design options in Chapter III.

## 2.1 Legal Nature, Scope and Drawbacks of FRIA under Art. 27

### 2.1.1 The Legal Character and Content Requirements

Article 27 of the AI Act establishes an obligation to a limited group of deployers to conduct, before deployment, an organized evaluation of the effects on fundamental rights that the deployment of a high-risk AI system may have. The FRIA is not a voluntary requirement: Article 27(1) states that the deployer "shall perform an assessment of the impact on fundamental rights". As stated before, it is an *ex ante* obligation which implies that it should be fulfilled before the deployment, but not as a reaction to perceived damage. It is also a requirement that stipulates a procedure of assessment, not the substantive result, meaning it does not, for instance, forbid deployment when fundamental rights risks have been found, and certainly does not provide a standard of harm under which deployment would be unlawful. This provision is thus, so far, an evaluation of the potential impact that any AI system may have on the rights of any individual that may be affected by the functioning of such system, without further specifying what the outcomes of identifying such substantial effect are. As Gill-Pedro establishes through a teleological and contextual analysis of the AI Act's legal basis under Article 114 TFEU, this obligation functions as a minimum harmonization standard: deployers may conduct more extensive assessments than Article 27 requires, or may initiate FRIAs in circumstances where the provision imposes no obligation to do so,[87] but EU law creates no duty on any deployer to exceed the statutory floor - with the structural consequence that the enacted minimum operates, in practice, as the effective ceiling for the majority of those subject to it.

The doctrinal parallel is the Court's distinction in Keck and Mithouard between product requirements and selling arrangements.[88] The FRIA obligation operates as the rights-assessment equivalent of a selling arrangement: it regulates how an AI system is deployed, not what it contains, and leaves Member States and deployers free to go further.

Article 27(1) outlines six substantive elements that the FRIA should include. The deployer must provide: (a) a description of the deployer’s processes in which the high-risk AI system will be used in line with its intended purpose; (b) a description of the period of time

[87] Ibid., §§3.2-3.3, 11-15.
[88] Joined Cases C-267/91 and C-268/91, Keck and Mithouard, ECLI:EU:C:1993:905, §§14-17.

within which, and the frequency with which, each high-risk AI system is intended to be used; (c) the categories of natural persons and groups likely to be affected by its use in the specific context; (d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13; (e) a description of the implementation of human oversight measures, according to the instructions for use; (f) the measures to be taken in the case of the materialization of those risks, including the arrangements for internal governance and complaint mechanisms.

It must be mentioned that, as it is, current enumeration is more descriptive rather than evaluative: elements (a), (b), and (c) only demand a factual description, whereas element (d) only demands the identification of risks based on the information that has already been provided by the provider. The evaluation is consequently anchored to how the provider frames the capabilities and limitations of the system as opposed to assessment being independent. Additionally, element (e) on human oversight directly refers to the "instructions for use" - the deployer is once more instructed to read the documentation of the provider, as opposed to being encouraged to independently determine whether or not adequate oversight measures are implemented in the particular deployment scenario. Lastly, the provision does not at all presuppose an evaluation of either the proportionateity or necessity of deployment in the situation, and certainly not the mitigability of the identified risks.

These content requirements, without accompanying methodological guidance, are inadequate. The AI Act itself is not enough to describe the implementation of a FRIA, as no parameters are mentioned on how to implement adequate measurement paths and no complete tools have been put in place.[89] The content requirements thereby establish minimum documentary standards without affording the normative or methodological scaffolding required to make sure the minimum documentary standards yield actual rights protection.

### 2.1.2 The Temporal Dimension

This disadvantage is not removed, but only aggravated by the very temporal structure of Article 27, further complicating substantive requirements that are already insufficient.

The temporal structure of Article 27 embodies the overall *ex ante* logic of the product-

[89] Lucilla Gatt, Ilaria Amelia Caggiano, Maria Cristina Gaeta, Emiliano Troisi, Roberta Savella, Francesca Pratesi, and Roberto Trasarti, 'FRIA Implementation Model According to the AI Act,' *European Journal of Privacy Law & Technologies* 2 (2024): 193-194.

safety model of the AI Act, but adds some complexity to its extension to deployer obligations. Article 27(1) requires assessment prior deploying of the high-risk AI system, setting the FRIA as a pre-deployment requirement, and not a long-term monitoring exercise. Article 27(2) then specifies that the obligation laid down in paragraph 1 applies to the first use of the high-risk AI system, meaning that later applications can be covered by a prior assessment.

The initial principles on the DPIA under the GDPR, laid down by the Article 29 Data Protection Working Party by analogy stated that a DPIA is the process which is intended to describe the processing, evaluate its need and reasonableness and assist to deal with the risks to the rights and freedoms of natural persons, and the execution of DPIA is not a one-off event but a constant activity.[90] The Article 27 FRIA, on the other hand, does not recreate the GDPR obligation of the continuous review in the literal sense. Neither the body of Article 27 nor Recital 96 state that the FRIA has to be revised where there are material changes in deployment context, affected population or risk landscape. In its Opinion 44/2023, the EDPS noted that the certification of AI systems should not be treated as a 'one off' exercise and must be an ongoing process, but yet this is not reflected in the FRIA in the AI Act.[91] The consequence is a temporal gap: a FRIA that was completed at the time of the first deployment may become normatively obsolete to the development of the usage of the system, without necessitating the reevaluation. This temporal inflexibility stands in direct contrast to the iterative model that the HRIA tradition requires - a tradition in which, as Section 1.4 established, assessment is designed as a continuous, multi-phase process precisely because rights impacts emerge, compound, and evolve through the deployment lifecycle rather than fully preceding it.

The temporal inflexibility counters the very nature of the risks that Article 27 is designed to address. Lasek-Markey and Hogan imply that Article 27's pre-deployment snapshot model is insufficient - the HRIA tradition requires participation 'at points in time' throughout deployment, and Mantelero's template demands 'adaptability to evolving technological and societal dynamics,' neither of which Article 27 mandates.[92] The framework of the AI Act, based on the product safety paradigm of pre-market compliance certification and further market surveillance, does not suit the dynamic nature of AI-mediated harm - a temporal structural weakness that compounds the content deficiencies identified in Section 2.1.1 and that Section

[90] Article 29 Data Protection Working Party, Guidelines on DPIA, 4, 14.
[91] "Opinion 44/2023 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act)," European Data Protection Supervisor, Brussels, 2023, 19, §61.
[92] Lasek-Markey and Hogan, Delivering on the Promise, §5.1.

2.5 measures against the iterative benchmarks of the HRIA and DPIA traditions.

### 2.1.3 The Critical Scope Limitation

One of the flaws of the FRIA practical application may be the limitation of its scope, introduced in Article 27(1). The Article states that:

"Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, **deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III (**which concern access to private essential services such as insurance and banking**)**, shall perform an assessment of the impact on fundamental rights that the use of such system may produce."

The implication of the scope limitation in practice is that private companies are required to perform an impact assessment only when they are implementing high-risk systems as mentioned in Annex III(5b)... and (5c). The very vast majority of deployers in the private sector, even those deploying systems officially specified as high risk under Annex III, are thus not subject to the FRIA requirement at all. This scope constraint then results in the paradox of a rights-assessment regime where most rights-impacting deployments are not subject to the regime.

The teleological analysis of Gill-Pedro accentuates this criticism. He shows that the AI Act puts the free movement of AI systems ahead of the overall protection of fundamental rights and that, as adopted, the FRIA has a high market bias.[93] The scope restriction is not a by-product of drafting style - it is an expression of choice to put the burden of rights-assessment to the public sector. Regrettably, at this moment, the private parties that do not fall within the categories are subject to control, at best, through the pre-market conformity testing by the provider.

### 2.1.4 The Template Questionnaire and MSA Notification

For deployers who happen to fall under the narrow scope of Article 27, the statutory response to the methodological vacuum outlined above is two-fold: a template questionnaire through automated tool, which AI Office is yet to draft in order to ensure deployers meet their obligations under this Article - a solution which has also faced considerable methodological

[93] Gill-Pedro, Fundamental Rights Impact Assessments, §3.1.1, §3.1.3.

criticism.

Mantelero defines the risk most precisely, arguing that a simple questionnaire-based approach, much less an automated one, seems incapable of fully capturing the contextual nature of FRIA.[94] The inherent challenge is that as a tool in the HRIA tradition, the FRIA is based on the assumption endorsed by the FRA itself that fundamental rights compliance is not automatable and hard-coded into computer programmes. Instead, use cases should be analyzed individually.[95] Article 27(5) requires creating an automated tool to make compliance easier - but this actually contradicts the core idea behind FRIA, which says that fundamental rights compliance cannot be automated. This approach "fails to consider the contextual nature of fundamental rights assessment."[96] The questionnaire method also threatens to deliver what Binns in his review of the similar DPIA develops an exercise in legitimization instead of risk evaluation - evaluations that create conforming documentation without interacting with the normative substance of rights protection.[97]

A further critical omission compounds this methodological inadequacy: Article 27 contains no obligation to implement any identified mitigation measure prior to deployment. The six-element template of Article 27(1) requires the deployer to describe the measures to be taken "in the case of the materialisation of those risks" under Article 27(1)(f), but does not condition the lawfulness of deployment on the prior adoption of those measures - with the result that a deployer who identifies serious fundamental rights risks and records them in the completed questionnaire has formally satisfied Article 27, regardless of whether any corrective action is taken before the system is put into service.[98]

The three-block framework suggested by Mantelero in the literature — covering (1) planning and scoping with awareness raising and risk identification, (2) data collection and risk analysis, and (3) risk management, comprising the adoption of preventive or mitigating measures and iterative testing of their effectiveness - offers a more analytically rigorous framework; yet not a single word in Article 27(5) or the full text binds the AI Office questionnaire to reflect this or any similar structure. Notably, stakeholder participation in Mantelero's framework is not a discrete third block but a cross-cutting process criterion

[94] Mantelero, The FRIA in the AI Act, 9.
[95] FRA, Getting the Future Right, 87.
[96] Mantelero, The FRIA in the AI Act, 9.
[97] Binns, Data Protection Impact Assessments, 25.
[98] AI Act, Art. 27(1)(f).

applicable throughout all three phases - a design feature that Article 27 omits entirely.

This criticism is heightened by the fact that Article 27(3) refers to the finished questionnaire as a single tool whereby the deployer fulfils its notification duty to the competent authority. Article 27(3) obliges the deployer, after the FRIA has been conducted, to inform the market surveillance authority (MSA) of its findings, and include the completed template mentioned before as an appendix to the notification. This notification requirement has two important implications: it creates a formal point of responsibility between deployer and public authority and it designates the market surveillance authority, but not a data protection authority or fundamental rights body, as an institutional recipient of the results of FRIA.

Additionally, as Wachter notes, the FRIA does not need to be publicized - in other words the notification mechanism establishes institutional responsibility without transparency to the people affected or civil society.[99] The ECNL and SocietyInside guidance recognises transparency and access to information as being part of the criteria of a meaningful FRIA and that it is essential to empower affected persons and civil society to examine the results of the assessment.[100] The private notification model of Article 27(3) does not meet either of them.

Combined, Articles 27(5) and 27(3) generate a compliance architecture whose structural design is oriented towards formal completion instead of substantive protection. The questionnaire makes the evaluation easy and a fillable paper; the notification provides that paper to an authority and does not obligate the deployer to reveal that paper any further. What the two provisions together guarantee is that a deployer could meet the letter of Article 27 by filling out a form and submitting it - with no assurance that the underlying rights analysis is done with the methodological rigour that the tradition of HRIA would demand, or that it can be checked by interested persons.

#### 2.1.5 Sub-Conclusion 1

To understand the architecture of Article 27, it is necessary to be explicit on what Sections 2.1.1-2.1.4 have established that it omits. Article 27 prescribes no content threshold that would bar deployment where serious rights risks are identified, does not mandate publication of the FRIA or its results, and does not require that those performing the assessment

---

[99] Sandra Wachter, "Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond," *Yale Journal of Law & Technology* 26, no. 3 (2024): 683.

[100] European Center for Not-for-Profit Law (ECNL) and SocietyInside, *Civil Society Guidance on Fundamental Rights Impact Assessments under the EU AI Act* (Brussels: ECNL, 2023), 7.

possess basic competence in fundamental-rights methodology. The broader omissions (pre-assessment consultation, external verification, enforcement triggers, and continuing review) are developed in Sections 2.2 through 2.4.

These omissions are not technical but the result of a legislative compromise whereby, according to Mantelero, the FRIA provision was significantly limited in the trialogue.[101] The most consequential individual amendment was the elimination (as Mantelero records) of a previously proposed requirement to forego deployment where risk mitigation measures could not be identified. This requirement, had it been retained, would have aligned Article 27 with Wernick's normative standard that a genuine impact assessment must preserve the option to abandon the project as its most protective output.

Taken together, the findings of Sections 2.1.1 through 2.1.4 establish three of the seven structural weaknesses set out in the taxonomy of Section 2.6: the product-safety mismatch between the NLF's pre-deployment snapshot model and the iterative logic that genuine fundamental rights assessment requires; the scope limitation that positions the constitutional ceiling of Article 51(2) CFR at precisely the point where the majority of rights-impacting AI deployments occur; and the methodological vacuum produced by the absence of any normative or procedural framework governing the FRIA's conduct. The combined consequence is that Article 27, as enacted, is architecturally capable of producing formal compliance without substantive rights protection. It is this structural possibility that Sections 2.2 through 2.5 examine through the lens of the provider-deployer relationship, the enforcement architecture, and the comparative benchmarks of the HRIA and DPIA traditions.

## 2.2 Deployers and Providers: Roles, Obligations, and Structural Tensions

### 2.2.1 The Provider-Deployer Division: Obligations and Their Limits

The structural tensions of the provider-deployer relationship emerge at the definitional level: Article 3 of the AI Act establishes a division that, when applied to the FRIA architecture of Article 27, generates an information asymmetry in which the party that controls the technical knowledge necessary to assess rights impacts is not the party obligated to conduct the assessment.

The definitional Article 3 of AI Act states, that:

(3) ‘provider’ means a natural or legal person, public authority, agency or other body

[101] Mantelero, The FRIA in the AI Act, 7-8.

that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;

(4) 'deployer', on the other hand, means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;

Related Recital 13 additionally states that "the notion of 'deployer' referred to in this Regulation should be interpreted as any natural or legal person, including a public authority, agency or other body, using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity. Depending on the type of AI system, the use of the system may affect persons other than the deployer."

As Almada and Petit note, the majority of the duties associated with the AI Act are imposed on **providers** of high-risk AI systems,[102] who should guarantee compliance with the technical stipulations of the Act before the system can be brought to the market or brought into service and the product safety regulation has a functional justification in this division: the manufacturer (supplier) is most informed about the technical characteristics of the product, while the user (developer) can most effectively assess the operating conditions.

The primary mechanism through which providers meet this pre-market compliance condition is the conformity assessment - the process where a provider ascertains that a high-risk AI system meets the mandatory requirements of the Act before it is introduced to the market. The provider-based character of this obligation is, though, carried out in the very form of this assessment. For the second type of high-risk AI systems, those outlined in Annex III, Article 6(2) (primarily the ones impacting fundamental rights), Kaminski describes the resulting regime as "licensing 'ultra-lite'": the process of conformity assessment is devoid of any external third parties, instead consisting solely of internal self-assessment and review.[103] The consequence is that the substantive analysis of the presence of unacceptable risks on fundamental rights of a system is performed at the pre-market stage by the very party that stands to gain the most out of a favourable decision.

Wachter identifies this dynamic precisely: providers, as the dominant stakeholders in the CEN/CENELEC working groups that write the harmonized standards, play a central role in

[102] Almada and Petit, "The EU AI Act", 9.
[103] Margot E. Kaminski, "Regulating the Risks of AI," *Boston University Law Review* 103 (2023): 1381-1382.

creating those standards and then self-assess whether their systems comply with them - creating, as she writes, 'a major legal loophole in which those who are supposed to be regulated can testify to compliance with rules they have written for themselves'.[104]

This conflict of interest generates an information asymmetry at the heart of the FRIA architecture: the provider controls the technical documentation on which the deployer must rely when conducting the rights assessment under Article 27(1)(d), yet the provider's obligations under the AI Act run to product safety and internal market conformity - not to the protection of fundamental rights.

The outcome of this structural conflict of interest has a direct effect on the FRIA. In Article 27(1)(d) the assessment that a deployer conducts regarding certain risks of harm is specifically qualified by the instruction to take into account the information provided by the provider in accordance with Article 13. The rights assessment of the deployer based on the instructions of the provider to use the system and the technical documentation therefore is pegged on the prior characterisation of the system by the provider. It is not an administrative convenience, but a structural subordination of the rights evaluation of the deployer to the commercial framing of the provider.

On the other hand, the FRIA obligation puts the deployer in the role of rights protector, but the structural resources to discharge that role are minimal. Almada and Petit identify the core design issue: the AI Act's emphasis on market access produces technical requirements that are oriented towards procedural conformity, whereas the GDPR and the DSA are structured around the protection of specific substantive values - a methodological divergence that renders the AI Act's product-safety means structurally inadequate to its stated fundamental-rights ends.[105] With at most the instructions of the provider on use, a template questionnaire of the AI Office, and the substantive requirements of Article 27(1), the deployer is supposed to make a meaningful impact assessment on the entire spectrum of Charter rights - but with no methodological advice as to how rights are to be identified, weighted or traded off with other considerations, the provided tools are structurally inadequate to do the job.

The role of the deployer is further confounded by the fact that it is associated with persons whose rights are affected by deployment of high-risk AI system. The most notable difference in terms of historical context is the fact that despite the FRIA in the AI Act being

[104] Wachter, Limitations and Loopholes, 692.
[105] Almada and Petit, The EU AI Act, 12.

rooted in the HRIA tradition, they have failed to incorporate certain features of the model - the most prominent of them being the active involvement of the stakeholders in the assessment process.[106] According to Lasek-Markey and Hogan, the lack of requirement to consult with affected communities is one of the "technical" systemic flaws of Article 27 - distinct from the HRIA tradition that rights-assessment should be a process in which rights-holders are active agents, not passive objects.[107] Against the five HRIA criteria set out in Section 1.4, and in particular the process-side requirement of stakeholder participation, Article 27 imposes none of them on a mandatory basis. The deployer is supposed to protect rights on behalf of people that might be never consulted.

The legal nature of the deployer's obligation is thus not that of a true rights assessment in the HRIA sense (which is based on stakeholder participation, independent review, and methodological rigour), but in a systematic documentation requirement that is done in isolation, based on provider-framed technical information, without consultation of the affected parties, nor with the normative instruments needed to identify, weigh, or trade off rights. This is what Mantelero describes as a risk of turning the FRIA into a descriptive exercise, as opposed to a real rights assessment.[108]

This participation gap constitutes the factual predicate for Design Option 4 in Chapter III and corresponds to the participatory component of the structural weaknesses synthesized in Section 2.6.

Consequently, the provider-deployer division, as currently designed by the AI Act, fails to establish two layers of rights protection, but establishes a layer of provider-based technical conformity and a layer of deployer-based documentation - neither of which seem to be a real fundamental rights evaluation tool.

### 2.2.2 The Reliance Mechanism and Territorial Scope

Article 27(2) permits that the deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by the provider.

The reliance mechanism works in two directions. First, it allows a deployer to replace a previous FRIA by itself with the one it has already completed under similar conditions.

---

[106] Mantelero, The FRIA in the AI Act, 16.
[107] Lasek-Markey and Hogan, Delivering on the Promise, §5.1.
[108] Mantelero, The FRIA in the AI Act, 9.

Second, and more importantly, it allows the deployer to draw on an existing impact assessment by the provider. The second limb is more important: the pre-market documentation, made by the provider, is - as it has been established above - a product safety tool produced by an economically interested party that has not been independently verified, yet is under Article 27(2) a functionally substitute alternative to the context-specific rights assessment of the deployer.

Reliance on the providers' documentation under Article 27(2) is likely to make the FRIA a document-management exercise, instead of an actual rights assessment. The point is structural: in case the deployer chooses the reliance option, the FRIA breaks down into reviewing the prior documentation of the provider. The contextual specificity - the defining virtue of a deployment-stage rights assessment, i.e. the capability to assess impacts in the context of the particular organisational, demographic, and operational conditions of deployment - is substituted by a generic prior assessment. This tension was anticipated by the EDPB and EDPS in their Joint Opinion 5/2021, noting that the assessment performed by the provider would be of a more general nature than that of the deployer, whereas the latter would be context-specific yet less informed, due to the limited access of the deployer to the internal design of the system.[109] The reliance mechanism resolves this tension by permitting the deployer to defer to the generality of the provider, at the cost of losing contextual specificity in favor of actual rights analysis. This is the mechanism through which the formalistic compliance pathology that the thesis identifies is most directly produced: where the reliance option is exercised, the deployer's legally sufficient act under Article 27 is the review of a pre-existing document - not the conduct of an independent, context-grounded rights assessment.

The "similar cases" condition is not defined in the regulation, and it is not accompanied by any hint of the extent of contextual similarity that would be used to rely on it. With no methodological standards, the condition will be virtually unenforceable and will be read generously - further undermining the independence of the FRIA. These structural inadequacies of Article 27 - the dependence of the assessment of the deployer on the framing of the provider, the lack of methodological direction, the interpretive openness of the mechanism of reliance - do not, however, act alone. They are complicated by one more dimension: by whom, in what geographical and institutional area, the FRIA obligation applies

[109] "EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," European Data Protection Board and European Data Protection Supervisor, Brussels, 18 June 2021, 9, §§20-21.

at all. The discussion that follows explores the interplay of the broad territorial ambition of the AI Act with the narrow personal scope of Article 27, and the implications thereof to the ability of the FRIA to act as a real rights-protection tool outside of EU territory.

Article 2 of the AI Act establishes a broad territorial scope of providers and deployers in the EU, providers located outside of the EU, but the output of whose systems is used in the EU, and importers/distributors located in the EU. The seemingly ambitious nature of such scope is to make sure that the safeguards of the AI Act, such as the FRIA requirement, are applicable in cases where the citizens of the EU are harmed by the deployment of high-risk AI. Practically, though, the territorial scope of Article 27 is, to a large extent, offset by the scope restriction discussed previously: only public law authorities, private businesses offering public services and the particular deployers of the Annex III(5) (b)/(c) must undertake FRIAs. The geographical area of the rule is wide but the individual area of the FRIA liability is small.

#### 2.2.3 Sub-Conclusion 2

This analysis reveals that the provider-deployer division established by the AI Act fails to create two complementary layers of rights protection. It introduces, rather, an overlay of dependency: a layer of provider-imposed technical compliance, conducted by an economically interested party without independent verification, and a layer of deployer-imposed documentation, without methodological direction, consultation with stakeholders, and based on provider-framed technical information. This structural configuration constitutes the 'informational dependency' weakness - one of the seven structural weaknesses identified in the taxonomy of Section 2.6 - and is addressed in Section 3.2 through design options that impose mandatory information-sharing obligations on providers, introduce independent verification requirements, and ground the deployer's assessment in rights-specific methodological standards rather than product-safety documentation.

### 2.3 Liability and Enforcement Architecture

Article 99 of the AI Act establishes the administrative sanctions regime for non-compliance with the regulation. Article 99(4) lists non-compliance with obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), notified bodies (Articles 31, 33, 34), and transparency obligations (Article 50) as the penalty category.

The missing element in Article 99(4) is critical in current context: Article 27 is not mentioned in the list of the provisions the violation of which entails the Article 99(4) penalty

category. Article 26 legislative text enumerates certain deployer requirements in 99(4)(e), but does not include the FRIA requirement of Article 27 in the same category of penalty. This omission is analytically significant beyond its technical dimension: as Section 1.4 established through Götzmann's fifth criterion, a genuine rights-assessment instrument must be embedded in an accountability structure that identifies duty-bearers and provides access to remedy - and by placing Article 27 outside the Article 99(4) penalty schedule, the AI Act severs the FRIA from precisely that enforcement architecture.

The enforcement architecture of Article 27 produces four discrete gaps, each of which independently severs the FRIA from the accountability structure that Götzmann's fifth criterion requires.

Gap 1 - Penalty Exclusion: This seemingly minor omission has great enforcement connotations. The absence of Article 27 in the Article 99 penalty schedule leaves the enforcement basis of FRIA violations indeterminate. In his work about the risk management framework in the AI Act, Schuett anticipates that administrative fines to be considerably less than the upper limit, like those in the GDPR, based on some comparative experience in similar product safety penalties.[110] When FRIA violations receive less severe penalties or need to be enforced under the general residual penalty provision, the deterrent effect of the sanctions regime in cases of rights-assessment failures is correspondingly diminished. It is not just a technical deficiency in drafting, but reflects a broader structural condition of AI enforcement. Massive firms, as Malgieri and Pasquale note, face fines on AI misuses that are the economic equivalent of a parking ticket, a relationship that makes the financial sanction structurally insufficient as a compliance incentive for large-scale deployers.[111]

Gap 2 - Quality-Blind Supervisory Review: The enforcement regime of the AI Act is addresses the existence, as opposed to adequacy, even where sanctions are available. When the FRIA is notified under Article 27(3) of receiving the template submitted, the MSA has the power to examine the submitted template - but neither Article 27, nor the market surveillance provisions, broadly provide a means through which the MSA should be able to demonstrate that the substantive content of the FRIA has been reviewed in a way that is methodologically sufficient, factually accurate, or rights-protective in its effects. The AI Act in itself is, therefore,

[110] Jonas Schuett, "Risk Management in the Artificial Intelligence Act," *European Journal of Risk Regulation* 15, no. 2 (2024): 17.
[111] Gianclaudio Malgieri and Frank Pasquale, *From Transparency to Justification: Toward Ex Ante Accountability for AI*, SSRN Working Paper (2022), 2.

not enough to stipulate the implementation of a FRIA effectively, since there are no suggested parameters of the implementation of appropriate measurement paths. Without compulsory quality requirements, formal compliance and real rights evaluation are no longer linked: a deployer can meet its Article 27(3) notification requirement by filing a completed template that is nonetheless entirely inadequate as an evaluation of the impact on rights. From an enforcement standpoint, an unduly performed FRIA (one that reproduces provider documentation without contextual adaptation or records risks without analysing their rights implications) is legally equivalent to a rigorously conducted one: both satisfy Article 27(3)'s notification requirement, and neither triggers any adverse legal consequence beyond it. Black and Baldwin's general insight that "regulators can never rely on the firms' own systems either for implementation or for undistorted feedback or results" applies with particular force here: the FRIA is a self-assessment tool reviewed by a market surveillance authority ill-equipped to assess its substantive quality.[112] According to Toner, such a pathology has been found by the impact assessment in EU law: where there is an almost exclusively documentary obligation and a purely formal enforcement law, the impact assessment is likely to produce a tick-box mentality where procedural compliance replaces a substantive protection of rights - conditions that the architecture of Article 27 nearly ensures are met almost by default.[113]

Gap 3 - Absence of Prior Consultation Trigger: The enforcement deficit is equally strong at the procedural level. A key structural difference between the FRIA and the rights-assessment framework of the GDPR is that the former does not include a similar mechanism to the GDPR Article 36 prior consultation. Article 36 GDPR states that, in the case where a DPIA states that processing would cause a high risk that the controller cannot address, the controller should first seek advice from the supervisory authority, before commence processing. The FRA has highlighted this mechanism as providing a crucial role to DPAs, as independent bodies established by law in ensuring that residual high-risk processing is subject to external scrutiny before it proceeds.[114] Article 27 contains no analogous provision. There is no mechanism by which a deployer that identifies, through its FRIA, unmitigable risks to fundamental rights is required to halt or refer the deployment. The previous consultation requirement has, as the Article 29 Working Party formulated in its DPIA-purpose, a decision-forcing purpose: the

[112] Julia Black and Robert Baldwin, "Really Responsive Risk-Based Regulation," *Law & Policy* 32, no. 2 (2010): 19.
[113] Helen Toner, "Impact Assessments and Fundamental Rights Protection in EU Law," *European Law Review* 31, no. 3 (2006): 12.
[114] FRA, Getting the Future Right, 89.

assessment becomes a prospective point of control that can block the processing before it happens and is harmful.[115] In the absence of a similar mechanism in Article 27, the FRIA is prospective in nature but has no consequence in procedure. A deployer can fill in a comprehensive FRIA, recognize extreme threats to core rights and deploy without any hindrance - thus meet the letter of Article 27 but break its spirit.

Gap 4 - Incompleteness of Individual Remedies: Individual enforcement is equally incomplete. Article 86 of the AI Act lays down a right to explanation to persons who are the subject of decisions made based on the output of high-risk AI systems - the only individual-facing enforcement of the Act itself. The AI Act does not give any right to appeal, overturn, or compensate for a decision, but the affected person may request an explanation of the decision. The description of how the AI system came up with a decision does not, in itself, prove that the decision infringed the fundamental rights of the person, nor does it constitute the cause of action of the infringement under the framework of the AI Act. The AI Liability Directive, a proposal to enable civil redress for harm caused by AI, was intended to complement the AI Act in this regard, but the legislative development of that bill has been questionable and the interaction with the compliance architecture of the AI Act has not been established yet. The gap that Article 86 cannot fill alone may be found in the characterisation of the binary governance model by Kaminski, where he states that both the individual due process rights and the systemic collaborative governance are necessary as complementary factors.[116]

The four gaps identified above converge on a single structural diagnosis: Article 27 violations fall outside the penalty schedule; the MSA notification mechanism verifies existence but not quality; no prior consultation trigger converts identified risks into deployment constraints; and individual enforcement addresses explanation rather than remedy, while the private enforcement landscape remains incomplete. Black and Baldwin demonstrate that risk-based frameworks are "not neutral, technical instruments" and that "risk analyses offer little assistance in relation to many of the familiar problems that regulators face - such as how best to secure compliance."[117] The FRIA of the AI Act works precisely in this area: it is concerned with formal adherence to organized evaluation processes but does not delve into the underlying issue of how compliance with the requirement can be translated into the practical safeguarding

[115] Article 29 Data Protection Working Party, Guidelines on DPIA, 18-19.
[116] Margot E. Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability," *Southern California Law Review* 92 (2019): 1529.
[117] Black and Baldwin, Really Responsive Risk-Based Regulation, 5, 12.

of the fundamental rights in particular deployment situations. The structural enforcement deficit is not a contingent failure of implementation, but a predictable consequence of the design choices. Combined, the sanctions architecture, the lack of a sufficient quality gap in MSA supervision, and the lack of a prior consultation mechanism, in combination with insufficiency of individual remedies, do not just reflect the isolated technical failures, but represent a patterned trend, in which the FRIA obligation is systematically shielded from the mechanisms that would otherwise be needed to render it operational. The outcome is an enforcement architecture which guards the semblance of rights assessment without assuring its content. The design options developed in Section 3.2 respond to each of the four enforcement gaps identified in this section (the penalty vacuum, the quality-blind MSA review, the absence of a prior consultation mechanism, and the incompleteness of individual remedies) through accountability-centred design features absent from the current Article 27 framework.

### 2.4 Market Surveillance Authorities and National Governance

The institutional dimension of the FRIA begins with the Article 27(3) notification mechanism. Under this provision, the deployer notifies the market surveillance authority (MSA) of the FRIA's results, submitting the completed template questionnaire as part of the notification. The MSA is the competent authority designated under Chapter IX of the AI Act and, in most Member States, is likely to be an existing product safety or standardisation authority.

The structural choice of MSA to receive FRIA notifications has far-reaching consequences. MSAs are constituted, resourced, and experienced in assessing products against technical safety standards - a role, which is categorically distinct to assess the effects of an implemented AI system on a variety of fundamental rights across a specific population. This argument was explicitly made by the EDPS in Opinion 44/2023, which asserts that data protection authorities are in a better position to handle complaints from persons who are affected by the use of the AI system because the market-surveillance authorities are market-focused.[118] This institutional critique of the EDPS is correct: a market surveillance authority is fundamentally not competent to determine whether a deployer is complying with the right to non-discrimination, the right to an effective remedy, or the rights of the child - matters that involve expert rights knowledge, the one that product safety regulators cannot generally have.

This institutional critique is reinforced by a structural resource gap. Many

[118] EDPS, Opinion 44/2023, 16, §49.

organizations might not have the capabilities necessary to conduct rights-competent assessment,[119] and the same statement can be made with respect to the regulatory bodies that are likely to be in charge of such assessments. In Opinion 44/2023, the EDPS recognised that undertaking the functions envisaged of a national AI supervisory authority will need the special expertise and resources - a statement which constitutes an admission that the resources themselves are not yet available in the scale needed.[120]

Schuett observes that Article 9 lacks any requirement to evaluate the effectiveness of the risk management system itself, and that its organizational dimension is underdeveloped.[121] MSAs, which operate within this framework, get FRIA notifications without an explicit defined authority to determine whether the underlying assessment was done competently, the correct risks are identified, and the mitigation measures proposed are appropriate. The notification process is therefore an administrative filing requirement as opposed to a real supervisory checkpoint.

This limitation operates at the institutional level in the same way that the Article 99 penalty gap identified in Section 2.3 operates at the sanctions level: both mean that the FRIA can be formally completed without triggering any legal consequence for its substantive inadequacy. The asymmetry is structurally embedded in the MSA's legal powers. Under Article 74 of the AI Act, MSAs may require a deployer to produce the completed FRIA documentation for inspection - the power to access the record exists.[122] What Article 74 does not authorise, however, is any power to require a deployer to improve the substantive quality of an assessment that has formally been completed: once the template questionnaire has been submitted, the notification requirement is satisfied and the MSA's primary statutory intervention point is exhausted. Equally, MSAs have no authority under the AI Act to order pre-deployment suspension on the ground of FRIA inadequacy - that corrective power is reserved for non-compliance with the system-level requirements of Articles 5 and 6, not for the procedural rights-assessment obligation of Article 27. The result is that an MSA can receive, file, and even examine a FRIA that is wholly inadequate as a rights-assessment instrument - but cannot compel the deployer to redo it, improve it, or submit it to review by a rights-competent authority.

---

[119] Theodoros Karathanasis, *The FRIA in EU AI Act: Governance, Rights, and Global Jurisdiction*, SSRN Working Paper, 5 July 2025, 8.
[120] EDPS, Opinion 44/2023, 18, §59.
[121] Schuett, Risk Management in the AI Act, 18.
[122] AI Act, Art. 74(1)-(2), Art. 79(1).

Further institutional complication is that of the jurisdictional overlap between MSAs and data protection authorities (DPAs). Article 27(4) sets out the relationship between the FRIA and the DPIA under the GDPR explicitly stating that in the event that DPIA obligations are already satisfied, the FRIA shall complement the DPIA. This complementarity mechanism assumes some institutional coordination between the MSA (the recipient of FRIA) and the DPA (the overseer of DPIA). In practice, though, the two groups of institutions are governed by different legal structures, have varying cultures of supervision, different enforcement capacities, and, as the EDPB/EDPS Joint Opinion 5/2021 contended, different competences.

The Joint Opinion urged that DPAs should serve as national supervisory authorities for the AI Act, rather than MSAs, on the grounds of existing expertise in rights-impact assessment.[123] The adopted AI Act rejected this recommendation. The result is a bifurcated supervisory architecture in which the DPA oversees the DPIA and the MSA receives the FRIA, with no structural mechanism to ensure that the two institutions share information, coordinate assessments, or resolve conflicts where a deployer's documentation addresses data protection impacts separately from broader fundamental rights impacts. In practice the Data Protection Officer (DPO) is likely to play key role in FRIA processes but may lack FRIA-specific expertise beyond data protection - an observation that points precisely to the institutional gap at the deployer level that mirrors the DPA-MSA gap at the supervisory level.[124]

These institutional conflicts are aggravated by the governance implications of co-regulation and standardisation for the FRIA.

The AI Act does not specify the approach for compliance with its requirements. It instead leaves the development of technical rules to European Standardisation Organisations (ESOs) - industry based bodies with membership dominated by large commercial interests and rather than fundamental rights experts. This delegation poses a structural risk of regulatory capture, through which the entities whose systems are the subjects of FRIA, effectively establish the standards on the basis of which compliance will be evaluated.[125]

The consequence of this is the following paradox: harmonised standards, as they are mentioned in the Official Journal, are given a quasi-legislative effect - adherence to them leads to a legal presumption of conformity with the AI Act. Yet these very standards are in fact private

[123] EDPB and EDPS, Joint Opinion 5/2021, 3.
[124] Ajoodha and Browne, Fundamental Rights Impact Assessments, 8.
[125] de Vries, Kanevskaia, and de Jager, Internal Market 3.0, 596, 603.

rules developed in a process where commercial interests have been systematically overrepresented[126] as shown by composition of the AI High-Level Expert Group, which included only 4 ethicists among its 52 members.[127] The methodology of fundamental rights, which must regulate both types of provider conformity assessment and deployer of FRIAs, is thus influenced, in the former case, by institutions who lack the authority, the expertise, and the independence to pursue rights protection as a substantive legal purpose - and which, by disposition and design, tend to reduce it to a "procedural tickbox".

The implication for the FRIA is straightforward. The substantive standards by which a deployer assesses the effects of fundamental rights, and by which an MSA determines the sufficiency of such assessment, are products of this captured standard-setting process. The co-regulatory architecture, together with weak mandatory content requirements of Article 27 and the unspecified template questionnaire of Article 27(5) generates the circumstances of a depoliticization of fundamental rights - in which normative decisions regarding the scope, weight, and trade-offs of rights protection are not debated in democracy and absorbed into technocratic compliance processes. The combined effect of the MSA-DPA bifurcation, the capacity deficit, and the standard-setting capture identified in this section constitutes the 'institutional misfit' weakness (the fourth in the taxonomy of Section 2.6) and is addressed in Section 3.2 through design options including mandatory DPA co-oversight of FRIA notifications, independent rights-competent audit requirements, and reform of the ESO standard-setting process to ensure fundamental rights expertise is represented.

### 2.5 FRIA, HRIA, and DPIA Interaction

The regulatory space of the deployment of high-risk AI now has three different assessment obligations that overlap: the HRIA, which is the methodologically-richest tradition (conceptually discussed in Chapter I); the DPIA under Article 35 GDPR; and FRIA under Article 27 AI Act. These instruments have a formal family resemblance: each is an *ex ante* structured assessment of possible harm, but varies in the conditions under which they are triggered, their substantive scope, the architecture of processes, and the institutional responsibility involved. The analytical base of the discussion below is to be based on a

[126] Marion Ho-Dac, "Considering Fundamental Rights in the European Standardisation of Artificial Intelligence: Nonsense or Strategic Alliance?" in *Joint Proceedings EURAS & SIIT 2023: (Responsible) Standardisation for Smart Systems*, ed. Kai Jakobs (2023), 3, 12, 18.
[127] Ronit Justo-Hanani, "Risk-Based Approach to EU AI Act: Benefits and Challenges of Co-Regulation," *Policy Design and Practice* 9, no. 2 (2026): 5-6.

comparative mapping of these instruments.

Table 1 below compares the three instruments in six dimensions that are essential for evaluation of a rights impact assessment quality: the scope of rights addressed, the circumstances under which the obligation is triggered, the extent of stakeholder participation, the consequences to adverse findings, whether the methodology is well-guided, and the supervisory institution. Combined, these dimensions demonstrate the structural distance between the FRIA as currently enacted and the norms that the HRIA tradition and, to a smaller degree, the DPIA regime have put in place as a precondition to an effective evaluation of effects on fundamental rights.

**Table 1: Comparative Assessment - FRIA, HRIA, and DPIA**

| **Criterion** | **FRIA (Art. 27 AI Act)** | **HRIA (UNGPs / Best Practice)** | **DPIA (Art. 35 GDPR)** |
|---|---|---|---|
| Scope of rights | All Charter rights (in principle) | All international human rights | Data protection rights and 'rights and freedoms' |
| Trigger | Prior to deployment - specific deployer categories only | Context-defined (project-based) | Where processing 'likely results in high risk' |
| Stakeholder participation | Not required | Required throughout process | Consultation of data subjects 'where appropriate' |
| Outcome constraint | No constraint - deployment may proceed regardless of findings | Deployment should be abandoned where residual risks cannot be mitigated | Processing must be suspended; prior consultation with DPA required where residual risk remains high (Art. 36 GDPR) |
| Methodological guidance | Template questionnaire (Art. 27(5)) | Rich academic and practitioner literature | Article 29 Working Party Guidelines |
| Institutional oversight | MSA (market surveillance authority) | Project-specific external reviewer | DPA (data protection supervisory authority) |
| Enforcement consequence | No penalty for substantive inadequacy | Project suspension / abandonment | DPA may prohibit processing |

Article 27(4) within this comparative context sets the formal interface between the FRIA and the DPIA. It states that in the case of DPIA duties under GDPR Article 35 or the Law Enforcement Directive Article 27 been fulfilled, the FRIA will supplement that data protection impact assessment. This formula of complementarity has an attractive logic - it implies a layered assessment architecture where data protection impact analysis and wider fundamental rights impact analysis are combined together - but its practical implementation is described vaguely almost to the verge of ambiguity.

The main issue is that Article 27(4) is supposed to supplement DPIA, not to substitute it, however, the complementary mechanism is not specified.[128] The provision gives no guidance on how the two instruments should be sequenced, how overlapping content should be handled, or how conflicts between the conclusions of a DPIA and a FRIA should be resolved. The distinction between the two instruments is categorical: in practice, most DPIAs primarily address impacts on data protection whereas a FRIA is meant to address impacts on all fundamental rights. Moreover, high-risk AI systems can have negative impacts that do not stem strictly from data processing, for example worker displacement due to new AI systems.[129] FRIAs and DPIAs are described as independent, distinct, yet complementary assessments, which suggests that they are institutionally and methodologically separate, rather than integrated as implied by the complementarity formula.

Empirical research establishes the basis for this concern: DPIA templates do not provide enough detail on rights other than data protection, and the GDPR does not provide specific rules on rights and freedoms other than data protection and even the data protection impact assessment enshrined in Article 35 needs specific implementation.[130] A FRIA that complements DPIA cannot merely be an extension of the DPIA analytical framework - it must have a very different conceptual framework. Another practical aspect supports this: although Article 35(1) of GDPR refers to “rights and freedoms”, implying that DPIA coverage is more comprehensive than data protection, guidance on DPIAs has mostly been limited to data protection, overlooking more fundamental aspects of rights.[131]

The Data Protection Officer is “likely to play key role” in FRIA processes, yet DPOs

---

[128] Mantelero, The FRIA in the AI Act, 9.
[129] ECNL and SocietyInside, Civil Society Guidance on FRIA, 6.
[130] Mantelero and Esposito, An Evidence-Based Methodology for HRIA, 10-11.
[131] Heleen Janssen, Michelle Seng Ah Lee, and Jatinder Singh, "Practical Fundamental Rights Impact Assessments," *International Journal of Law and Information Technology* 30, no. 2 (2022): 200.

"may lack FRIA-specific expertise" beyond data protection.[132] The complementarity model of Article 27(4) thus has the institutional implication of a FRIA by data-protection-trained professionals, relying on data protection-designed DPIA templates, in an institutional framework overseen by a market surveillance authority who lacks data protection expertise - whereas the DPA, which has expertise in both data protection and in any case part of the individual rights impact assessment, does not formally participate in the FRIA process. Binns' meta-regulatory analysis of the DPIA adds a further structural risk: where the DPIA that serves as the Article 27(4) baseline is itself susceptible to becoming a legitimization exercise (producing conforming documentation without substantive rights analysis) - a FRIA that formally 'complements' it inherits rather than corrects that vulnerability.[133]

In addition to this institutional misalignment, the comparison in Table 1 shows the size of the difference between the FRIA as implemented and the HRIA as theorized. The canonical HRIA taxonomy recognizes essential criteria to a methodologically sufficient impact assessment, grouped into process (grounding in international human rights standards, participation, non-discrimination, accountability, and - drawing on Lasek-Markey and Hogan's intersectionality framework - empowerment) and content criteria (comprehensive scope of impacts, assessment of impact severity including scope, extent and irremediability, the impact mitigation hierarchy of avoid-reduce-restore-remediate, and access to remedy). Article 27 meets none of the process criteria as binding requirements and only a portion of the content criteria in its six elements. Each of these process criteria corresponds directly to one of the four normative criteria established by Götzmann in Section 1.4 (grounding in international human rights standards, participation, non-discrimination, and accountability) supplemented by the empowerment dimension derived from Lasek-Markey and Hogan's intersectionality framework. Tested against this combined standard, Article 27 fails to satisfy any of them on a mandatory basis - a finding that identifies the 'methodological vacuum' and 'product-safety mismatch' as two of the structural weaknesses that the taxonomy of Section 2.6 names and maps to their design solutions.

Testing Article 27 against each of these five process criteria individually makes explicit the analytical basis for this conclusion:

[132] Ajoodha and Browne, Fundamental Rights Impact Assessments, 8.
[133] Binns, Data Protection Impact Assessments, 25-31.

Criterion 1 - International Human Rights Standards: Götzmann's first and foundational criterion requires that the assessment be anchored in internationally recognised human rights standards as the authoritative normative benchmark - in the EU context, the CFREU. Article 27 does not specify the CFREU or any other human rights instrument as the normative framework governing the assessment. The six elements of Article 27(1) require identification of affected groups and risks but impose no obligation to map those risks against specific Charter rights or to use international human rights law as the evaluative standard. The criterion is not met on a mandatory basis

Criterion 2 - Participation: Article 27 imposes no obligation to consult, engage, or obtain input from rights-holders or affected communities at any stage of the assessment process. The criterion is not met on a mandatory basis.

Criterion 3 - Non-discrimination: Article 27(1)(c) requires identification of affected categories and groups, but provides no methodological standard for intersectional analysis or for identifying differential impacts across overlapping dimensions of vulnerability. The criterion is formally addressed but substantively unenforceable.

Criterion 4 - Accountability (including transparency and access to remedy): As Section 2.3 established, Article 27 is excluded from the Article 99(4) penalty schedule; the MSA cannot compel substantive improvement; no prior-consultation trigger exists; the FRIA is notified to the MSA but is not required to be published or made accessible to affected persons, civil society, or the public; and individual remedies extend only to explanation, not redress. The criterion is not met.

Criterion 5 - Empowerment (Lasek-Markey and Hogan): The private notification model of Article 27(3) and the absence of any publication obligation mean that the individuals whose rights are assessed have no access to the FRIA's findings and no capacity to use those findings to assert rights or seek redress. The criterion is not met.

The criterion-by-criterion test confirms that Article 27's failure against the HRIA process standard is not partial or contextual but categorical: none of the five criteria (four derived from Götzmann and one from Lasek-Markey and Hogan) is satisfied as a binding requirement, establishing the methodological vacuum and product-safety mismatch as structural rather than incidental weaknesses

Most significantly, the HRIA's insistence on participation as a non-negotiable process criterion - operationalized in the HRIA literature by the observation that “consultation often

occurs when critical decisions have already been made" and that therefore rights-holder participation must occur "at critical points throughout the whole assessment process"[134] - finds no analogue in Article 27. This obligation of stakeholder consultation was diluted in the negotiation of AIA itself,[135] and the text adopted does not specify any obligation of any kind of participation. This exclusion is not only methodological but also political: with the removal of participation conditions, the normative decisions regarding the core rights are depoliticised by turning them into technical compliance practices carried out by the deployer without the participation of most affected individuals.[136]

The impact mitigation hierarchy, starting with harm avoidance and continuing with reduction, restoration, and remediation, does not have an organized counterpart in the content requirements of Article 27. The provision demands a description of what should be done in the event of the materialization of those risks (Article 27(1)(f)) which implies remediation at best, without the need to consider whether harm may be completely eliminated by way of design adjustment or abandonment of deployment. The seventh criterion of HRIA (scope of impacts) involves consideration of all types of rights impacts of all the affected groups; Article 27(1)(c) states that natural persons and groups that are likely to be affected are to be identified, but without methodological guidance on how that identification should be carried out across overlapping dimensions of vulnerability, the formal requirement may conceal substantial analytic deficiencies.

Mantelero's three-block model discussed in Section 2.1.4 (planning and scoping, data collection and risk analysis, and risk management) approximates the process requirements of the HRIA tradition, with stakeholder participation operating as a cross-cutting criterion throughout all three phases rather than as a standalone block.[137] Yet the reliance on the provider's documentation under Article 27(2) and the template questionnaire under Article 27(5) risks reducing even this model to its most attenuated form. Since in most cases the assessment is not based on measurable variables, the impact on rights and freedoms is necessarily the result of expert evaluation, where expert opinion relies on knowledge of case law, the literature, and the legal framework.[138] A questionnaire-based automated tool, however well designed, cannot replicate this form of expert legal judgment. The combined effect

[134] Götzmann, Human Rights Impact Assessment of Business Activities, 99.
[135] Wernick, Impact Assessment as a Legal Design Pattern, 23.
[136] Gill-Pedro, Fundamental Rights Impact Assessments, §3.4.
[137] Mantelero, The FRIA in the AI Act, 11.
[138] Mantelero and Esposito, An Evidence-Based Methodology for HRIA, 19.

(template questionnaire, provider-documentation reliance, and the absence of any mandatory methodological requirements) constitutes the 'methodological vacuum' - one of the seven-weakness of the taxonomy of Section 2.6.

The coexistence of FRIA, DPIA, and sector-specific assessment obligations without any structural integration mechanism (no sequencing rule, no conflict-resolution procedure, no shared institutional architecture) generates assessment fragmentation. The compliance burden is greatest for SME deployers, for whom the cumulative resource cost creates a structural incentive to substitute formal documentation for substantive rights evaluation. This is the 'assessment fragmentation' weakness in the taxonomy of Section 2.6.

A comparative analysis of the GDPR and AI Act risk-based approaches reveals a further tension: the GDPR's risk-based model is "concerned with better compliance," while the AI Act's risk-based model is "concerned with the determination of which AI systems should be regulated."[139] These are different regulatory functions and the instruments that are used to accomplish them - DPIA and FRIA, respectively, have different trigger conditions, procedural obligations and enforcement consequences. Considering them as complementary under Article 27(4) without considering these structural differences may lead to a hybrid instrument that does not do either of these functions satisfactorily. The findings of this section - Article 27's failure against each of Götzmann's four criteria, the methodological vacuum produced by the template questionnaire, and the assessment fragmentation generated by overlapping obligations - are incorporated into the seven-weakness taxonomy of Section 2.6, which draws on the findings of Sections 2.1 through 2.5 to produce the analytical bridge to Chapter III.

### 2.6 Conclusions of Chapter II

The analysis conducted in Sections 2.1 through 2.5 reveals that the structural limitations of Article 27 are not incidental but are the joint product of a single underlying condition: the placement of a fundamental-rights obligation within a regulatory instrument that is constitutionally grounded in Article 114 TFEU and architecturally designed around a product-safety model. This section synthesizes those analytical findings into a seven-point diagnostic taxonomy (drawing on the structural critiques identified in Sections 2.1 through 2.5) whose cumulative effect is to produce a legitimacy deficit at the heart of the FRIA obligation. Each of these seven structural weaknesses provides the design brief for Chapter III, where they are

[139] Gellert, The Role of the Risk-Based Approach, 1.

translated into a set of interdependent legislative and institutional design options for a Ukrainian FRIA-type mechanism.

The first weakness is the product-safety mismatch. The AI Act's Article 114 TFEU basis ties the FRIA to a product-safety architecture (pre-market conformity assessment, harmonized technical standards, and MSA supervision) whose methodological and institutional means are categorically ill-suited to rights protection; the deployer's rights-identification under Article 27(1)(d) is subordinated to the provider's commercial framing under Article 13, and the reliance mechanism of Article 27(2) permits a generic prior assessment to substitute for context-specific rights evaluation, embedding a structural conflict of interest at the operational core of the obligation.

The second weakness is the scope limitation. Article 27(1) restricts the FRIA requirement to public law institutions, private entities offering public services, and the designated Annex III(5)(b)/(c) deployers, while the vast majority of private-sector deployers of high-risk AI systems bear no FRIA obligation whatsoever, producing a legal incoherence whereby the same high-risk AI system triggers a rights assessment when deployed by a government agency but not when deployed by a private employer, where the underlying rights risks can be equally severe.

The third weakness is the methodological vacuum. Article 27 specifies the content of a FRIA but provides no guidance on how a deployer should identify, measure, or assess rights impacts against Charter standards; the Article 27(5) template questionnaire offers a documentary framework rather than a methodological one, and against the four process criteria of the HRIA tradition Article 27 fails to satisfy any as a binding requirement.

The fourth weakness is the institutional misfit. MSAs, designated as recipients of FRIA notifications under Article 27(3), are established and resourced for product-safety evaluation rather than fundamental rights supervision; the MSA-DPA jurisdictional bifurcation under Article 27(4) and the co-regulatory delegation of standard-setting to commercially-dominated ESOs compound this misfit by ensuring that the substantive standards against which compliance is evaluated are produced by institutions with neither the competence nor the independence to develop a genuine rights-assessment methodology.

The fifth weakness is the enforcement deficit. Article 27 is absent from the Article 99(4) penalty schedule, leaving its enforcement basis indeterminate; the MSA notification mechanism confirms the existence of the FRIA documentation but not its substantive quality;

and the absence of any prior-consultation trigger analogous to Article 36 GDPR means that a deployer may identify extreme unmitigated rights risks through its FRIA and proceed to deployment without any procedural restraint - with the result that the FRIA obligation is structurally decoupled from the accountability, remedy, and deployment-control mechanisms that Götzmann's fourth criterion requires.

The sixth weakness is assessment fragmentation. The coexistence of FRIA, DPIA, and HRIA obligations in the same regulatory space generates structural tensions that the complementarity formula of Article 27(4) does not resolve: the FRIA and DPIA differ in regulatory purpose, trigger conditions, and enforcement consequences, yet the AI Act provides no sequencing rule, no conflict-resolution procedure, and no shared institutional oversight architecture to integrate them; the resulting compliance burden creates a structural incentive to substitute formal documentation for substantive rights evaluation.

The seventh weakness is the participatory deficit. The absence of any mandatory obligation to consult, engage, or obtain input from the natural persons and communities whose fundamental rights may be affected by the deployment of a high-risk AI system produces a structural exclusion of rights-holders from a process that Article 27 formally designates as their protection mechanism. This is the feature most clearly at odds with the HRIA tradition's core methodological requirement that rights-assessment must be a participatory process in which rights-holders are active agents.

These seven weaknesses are mutually reinforcing in determinate ways. The product-safety mismatch (1) generates the methodological vacuum (3): a deployer evaluating provider-supplied risk information cannot reach beyond it without an independent rights-assessment methodology, and Article 27(5) supplies none. The methodological vacuum (3) compounds the institutional misfit (4): a market surveillance authority without a prescribed methodology has no analytical handhold by which to identify a defective FRIA, even when it has the documentation in front of it. The institutional misfit (4) reinforces the enforcement deficit (5): an authority that lacks the rights-competence to identify substantive inadequacy will not refer such cases for sanction, and the Article 99(4) penalty exclusion ensures that even if it did, no sanction would follow. The enforcement deficit (5) is amplified by the participatory deficit (7): rights-holders excluded from the assessment have no procedural channel through which to contest its inadequacy, and no remedy when they are harmed. The scope limitation (2) and the assessment fragmentation (6) operate as accelerators of the others: where the FRIA does not apply, the rights-protective architecture collapses to the DPIA alone (which by Section 1.4

cannot capture the full Charter rights spectrum); and where FRIA, DPIA, and HRIA obligations co-exist without a sequencing rule, the documentation-substitution effect identified in (5) intensifies. The seven weaknesses therefore constitute a single architectural failure, not a sum of seven independent ones - and a partial cure is structurally insufficient because each component depends on the others to produce its rights-protective effect.

These seven weaknesses are best seen not as distinct drafting mistakes but as mutually reinforcing consequences of an underlying structural conflict: Article 27 attempts to place a fundamental-rights function in a regulatory structure that is largely designed to integrate the market. What has been produced is a framework that offers more security to the form of assessment than to its substance. Chapter III shifts the focus to the implications of this diagnosis for Ukrainian law.

The orientation of Ukraine toward EU association and regulatory approximation puts pressure on convergence to the AI framework of the Union, and poses a legislative design question of its own: does approximation require the reproduction of the limits of Article 27, or can Ukraine, as a late adopter, impose FRIA-type obligations in a more robust and genuinely rights-protecting form.

# CHAPTER III

# IMPLEMENTATION OF A FRIA-TYPE OBLIGATION IN UKRAINE

The seven structural weaknesses of Article 27 of the EU AI Act identified in Section 2.6 are not merely a critical assessment but a design brief. These weaknesses define both the limitations and the prospects of the design task facing any jurisdiction that must approximate the fundamental rights impact assessment architecture of the AI Act. The approximation requirement defined in Section 1.3 provides the outer limit of that task, but not its internal structure. This chapter is a response to that architectural question. The combination of Ukraine's late-adopter status, its constitutional rights primacy, and the simultaneous legislative drafting of its data-protection and AI frameworks provides a design opportunity to adopt a FRIA mechanism that remedies the failures of Article 27 while fulfilling the approximation obligation. Section 3.1 maps Ukraine's existing constitutional and regulatory landscape against human rights impact assessment criteria and formulates a precise design problem. Section 3.2 draws on comparative models beyond Article 27 to develop seven design options for a Ukrainian FRIA mechanism. Each design option responds to one of the seven weaknesses identified in Section 2.6: constitutional anchoring (Option 1) addresses the product-safety mismatch (weakness 1); universal scope (Option 2) addresses the scope limitation (weakness 2); the prescribed three-stage methodology (Option 3) addresses the methodological vacuum (weakness 3); mandatory stakeholder participation (Option 4) addresses the participatory deficit (weakness 7); rights-competent supervision (Option 5) addresses the institutional misfit (weakness 4); binding enforcement with a prior-consultation trigger (Option 6) addresses the enforcement deficit (weakness 5); and integrated DPIA-FRIA design (Option 7) addresses assessment fragmentation (weakness 6).

## 3.1 Ukraine's Legislative Baseline

The regulatory baseline is reconstructed from Ukrainian constitutional text, draft legislation, and official policy instruments, read alongside the emerging scholarly analyses of Hura, Pavlenko, Perederii, and Yukhymenko; the Shevchenko et al. monograph on AI governance and the Ministry of Digital Transformation White Paper of June 2024 provide the most operationally detailed mapping of the field and are used as primary reference points within this broader source base.

Ukraine's approximation obligation under the EU-Ukraine Association Agreement encompasses the EU AI Act's FRIA architecture as part of the digital acquis that Ukraine has

committed to transpose.[140] As established in section 1.3, this obligation is binding and forward-looking. However, the obligation to converge at the normative level is not the same as an obligation to replicate the EU's specific constitutional architecture. Petrov demonstrates that the approximation clauses under the Association Agreement are binding in nature and prioritise regulatory convergence between the parties, establishing a functional standard that covers both existing and future EU legislation.[141] Komarova and Łazowski confirm that, following Ukraine's acquisition of EU candidate status, the approximation obligation extends to the entire EU acquis, yet remains result-oriented rather than form-prescriptive: Ukraine must achieve functional equivalence, not pure replication of EU legislative instruments.[142]

It might be objected that expanding the FRIA's personal scope to all private-sector deployers exceeds, rather than approximates, Article 27. The objection is misplaced: functional equivalence requires reproducing the protective effect of the EU instrument, not its politically compromised personal scope; a narrower Ukrainian FRIA would under-realise, not satisfy, the normative content the approximation obligation attaches to. The distinction between normative convergence and architectural replication is consequential for FRIA design, because it means that Ukraine is both bound to implement a fundamental rights impact assessment mechanism and free to design that mechanism within its own constitutional framework.

That constitutional framework provides a rights-primary foundation structurally unavailable to the EU legislature. The EU AI Act operates within an architecture where fundamental rights function as constraints on an internal-market integration project grounded in Articles 26 and 114 TFEU. Ukraine's Constitution inverts this hierarchy. Article 3 states that the human being, his or her life and health, honour and dignity, inviolability and security are considered in Ukraine as the highest social value and that human rights and their guarantees are the determinants of the content and direction of all state activity.[143] This is not merely a declarative preamble, but a structural command which puts the entire state action (including the regulation of technology) in the service of safeguarding individual rights.

Article 21 provides that rights are inalienable and inviolable; Article 22 is a non-

---

[140] Association Agreement between the European Union and its Member States and Ukraine, OJ L 161, 29 May 2014, Arts. 124, 394 and 474.
[141] Roman Petrov, "Approximation of Laws in the EU-Ukraine Association Agreement," *Naukovi Zapysky NaUKMA: Juridical Sciences* 155 (2014): 24.
[142] Tetyana Komarova and Adam Łazowski, "Switching Gear: Law Approximation in Ukraine After the Application for EU Membership," *Croatian Yearbook of European Law and Policy* 19 (2023): 117.
[143] "Constitution of Ukraine," Verkhovna Rada of Ukraine, adopted 28 June 1996, as amended [in Ukrainian], Art. 3.

regression clause, which forbids a reduction in the content and scope of the rights that exist when new laws are adopted.[144] Article 55 establishes justiciability by ensuring that all individuals have the right to appeal in court any decision, act or omission of the state authorities that infringe their rights.[145] The national AI Strategy itself recognizes this constitutional background, stating that the Strategy is based on the Constitution of Ukraine and is the foundation of all normative-legal acts related to AI.[146] Analyzing the implementation of the principles of the EU AI Act in Ukrainian context, the Ukrainian constitutional rights provisions are the main normative framework within which the AI governance mechanisms should be evaluated. The overall effect of Articles 3, 21, 22, and 55 is that any FRIA mechanism adopted under Ukrainian law must not consider fundamental rights as a factor in a cost/benefit analysis, but rather as the non-negotiable primary standard by which AI systems are judged - and any mechanism that allows only a 'box-ticking exercise' to be performed without real rights examination would be constitutionally impermissible (or, pending judicial review, at minimum constitutionally questionable) under the non-regression clause of Article 22.

The theory of 'rights as trumps' by Dworkin provides the philosophical architecture of operationalization of this constitutional position. According to Dworkin, individual rights are political trumps, which are possessed by individuals, and which can not be defeated by references to the general welfare or the aggregate utility.[147] This difference has direct operational implications to the design of FRIA: an assessment, based on Article 3 of the Ukrainian Constitution should not enquire whether a particular AI system is proportionate in a cost-benefit analysis, but whether it deprives individuals of rights they possess as trumps against the state and the commercial deployers. Dworkin then differentiates the rights-based and policy-based arguments, writing that rights claims have a qualitative priority that cannot be easily overcome by policy factors such as promotion of innovation or competitiveness in the market.[148] This conceptual framework defines the criterion for every design choice that will be outlined in section 3.2 - that a Ukrainian FRIA is a rights-legality check and not a proportionality optimization exercise.

The 'design corridor' that the Ukrainian Constitution creates also receives positive

---

[144] Constitution of Ukraine, Arts. 21-22.
[145] Constitution of Ukraine, Art. 55.
[146] Anatolii I. Shevchenko, ed., Strategy for Artificial Intelligence Development in Ukraine: Monograph (Kyiv: Institute of Artificial Intelligence Problems of the MES and NAS of Ukraine, 2023), 95-96.
[147] Norman E. Bowie, Review of *Taking Rights Seriously*, by Ronald Dworkin, *Catholic University Law Review* 26, no. 4 (1977): 908, 910.
[148] Bowie, Review of Taking Rights Seriously, 908, 914.

confirmation from EU law itself. The Corporate Sustainability Due Diligence Directive (CSDDD), adopted as Directive 2024/1760, demonstrates that mandatory rights-assessment mechanisms with binding stakeholder engagement are not structurally incompatible with the EU acquis, but already exist within it. Article 13 of the CSDDD requires companies, as a matter of law, to meaningfully consult affected stakeholders at specific points in the due-diligence process whenever they are identifying and addressing adverse human rights impacts.[149] Article 3(n), provides a wide definition of stakeholders, which includes not only commercial counterparties, but also the affected communities and civil society organizations.[150] This disproves any potential claim that a Ukrainian FRIA with identical or more stringent participatory guarantees would be incompatible with the EU. Although the CSDDD operates in a different regulatory domain, its participatory architecture shows that the EU legal order already accommodates mandatory rights-assessment consultation duties, and nothing in the AI acquis would render such duties structurally inadmissible in a Ukrainian FRIA regime. The CSDDD is examined further as a comparative design model in Section 3.2, where its participatory architecture is used to derive specific design options for a Ukrainian FRIA mechanism.

The design corridor can be summarized as follows: approximation determines the normative content that Ukraine should realise; the constitutional framework defines the rights-hierarchical architecture in which the content is executed. The two are not in conflict with each other-they help define the space where an architecturally superior FRIA can be constructed.

The further evaluation of the existing regulatory tools is organized around five categories, derived out of current human rights impact assessment practice (as outlined in Section 1.4) and modified to the constitutional provisions outlined above: (1) legally binding standard based on the rights identification; (2) institutional implementation and enforcement standard; (3) procedural participation standard; (4) scope covering the entire spectrum of rights that are interacted with by AI; and (5) post-deployment review cycle. These five categories adapt Götzmann's process criteria (Section 1.4) to the specific institutional and constitutional context of Ukrainian law: where Götzmann's criteria are process-oriented standards for evaluating an existing HRIA practice, the five categories used here are mechanism-design

[149] "Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859," *Official Journal of the European Union* L, 5 July 2024, Art. 13(1)-(3).
[150] CSDDD, Art. 3(n).

criteria for evaluating whether Ukraine's existing instruments provide the operational infrastructure a genuine FRIA requires. This diagnostic framework is indirectly embraced in the Concept of the Development of Artificial Intelligence in which the challenge of ensuring that AI systems are lawful and adhere to the current ethical standards is a problem that should be solved.[151]

The first regulatory instrument, the 2020 National AI Concept adopted by Cabinet of Ministers Resolution No. 1556-r, is a conceptually important agenda-setting document that defines the general direction of Ukrainian AI policy, but it does not yet translate this direction into concrete regulatory mechanisms. It incorporates the OECD principle that AI systems should be developed and used only in conditions that respect the rule of law, fundamental rights and freedoms, and democratic values,[152][153] and identifies the protection of rights and freedoms as the primary purpose of state policy in the field of AI legal regulation.[154] The National AI Strategy's three mandatory aims for 2023-2030 - to keep a record of ethical, legal and social consequences of AI use, to create mechanisms for ensuring ethical AI use, and to establish a thorough regulatory framework for the social relations brought about by AI technologies - together amount, in substance, to a functional description of FRIA-type objectives articulated in domestic policy terms.[155] However, in line with its nature as a conceptual policy act, the Concept itself does not establish a concrete assessment procedure, designate a supervisory authority, impose documentation duties on deployers, or provide an enforcement mechanism for those aims. As a result, the commitment to develop clear ethical and legal boundaries for AI development and implementation remains at the level of principles and planned directions, without specifying the subsequent legislative and institutional steps required to make those commitments operational.[156] European integration considerations and approximation to the EU AI acquis are also addressed only indirectly, despite scholarly warnings that delays in aligning with the EU framework may be detrimental to Ukraine.[157] Hura therefore characterises the existing Ukrainian AI regulation as disjointed, reactive and largely declarative - a diagnosis

---

[151] "On Approval of the Concept for the Development of Artificial Intelligence in Ukraine," Cabinet of Ministers of Ukraine, Resolution No. 1556-r of 2 December 2020, as amended by Resolution No. 1787-r of 29 December 2021 [in Ukrainian], section "Problems Requiring Resolution", 3.
[152] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (Paris: OECD, 2019, updated 2024), 8.
[153] Concept for the Development of Artificial Intelligence in Ukraine, 4.
[154] Ibid., 10.
[155] Shevchenko, ed., Strategy for Artificial Intelligence Development in Ukraine, 84-85.
[156] Concept for the Development of Artificial Intelligence in Ukraine, 11.
[157] Perederii, Legal Principles of AI Use, 58-59.

that captures the current distance between high-level commitments and concrete regulatory instruments.[158] From a human-rights-impact-assessment perspective, the Concept thus satisfies only the rights-identification dimension: it formulates relevant principles and objectives, but does not yet provide the institutional or procedural architecture needed to operationalise them as an HRIA- or FRIA-type mechanism.

The second regulatory instrument, The White Paper on Artificial Intelligence Regulation, which the Ministry of Digital Transformation released in June 2024, is a methodological improvement over the Concept. It recognizes the necessity of sequenced implementation and clearly recognizes a human rights impact assessment methodology as an important tool to prepare future national regulation and EU market access.[159] The White Paper proposes a two-stage approach: Stage 1 establishes voluntary compliance frameworks, while Stage 2 envisions mandatory, EU AI Act-aligned regulation.[160] Importantly, the White Paper documents the April 2024 meeting where EU representatives specifically directed the need to early transpose the EU Regulation into national law and that Ukraine should not leave the field of AI outside of any regulation in the interim.[161] Yukhymenko confirms that later involvement of Ukraine in the European Artificial Intelligence Board, formalised as of October 2025, represents the first step towards fulfilling the commitment of approximation as a binding, not aspirational obligation.[162] However, Stage 1 is voluntary - and a voluntary FRIA is analytically identical to no FRIA at all, as the deployers with the greatest incentive to run high-risk AI systems at scale are unlikely to face any legal penalty in the event of non-compliance. The White Paper is a roadmap, not a legal instrument - it satisfies at most one of the HRIA criteria (rights-identification, partially) while leaving the remaining unaddressed.

Third regulatory tool, Draft Law No. 8153 on Personal Data Protection, adopted in first reading, can become the most operationally-intensive AI-related rights instrument, yet so far its scope is constitutionally and functionally insufficient. Its regime of data protection impact assessment, enacted in Article 39, once adopted, will become the closest existing FRIA analogue in Ukrainian law: it is pre-deployment, risk-oriented and addresses processing that is likely to cause a high degree of risk to the rights and freedoms of natural persons.[163] Bodnar

[158] Hura, Adaptation to EU AI Act, 120, 122.
[159] "White Paper on Artificial Intelligence Regulation in Ukraine," Ministry of Digital Transformation of Ukraine, Kyiv, 2024, 19-20.
[160] White Paper on AI Regulation in Ukraine, 12, 18-19, 25-26.
[161] Ibid., 26.
[162] Yukhymenko, Analytical Note, 3.
[163] Draft Law No. 8153, Art. 39.

identifies DPIA for high-risk processing among the GDPR-aligned features of Draft Law No. 8153; it is the main procedural mechanism through which the data-protection standards take operational form.[164] Articles 40 and 41 also stipulate a prior consultation with the supervisory authority and appointment of a data protection officer - the procedural safeguards similar to what GDPR Article 35 mandates.[165]

However, as previously mentioned, the DPIA covers only the data-protection axis of fundamental rights. It does not consider all the range of rights that high-risk AI systems interact with: the right to a fair hearing, non-discrimination, dignity and bodily integrity, liberty, or the constitutional right to equal treatment in Ukraine as provided in Article 24 of the Ukrainian Constitution. According to Hura, systematic gap analysis shows that all the requirements related to Articles 9 to 15 of the EU AI Act (such as risk management systems, data governance, transparency, human oversight, accuracy, and robustness) are not reflected in Ukrainian law.[166] The AI Act's FRIA obligation under Article 27 imposes on specified deployers of high-risk AI systems an independent pre-deployment assessment duty that extends beyond the data-protection scope of the GDPR DPIA to encompass the full range of fundamental rights - an obligation that no existing Ukrainian legal instrument replicates.[167] The structural point is clear with the Dutch FRAIA approach: a DPIA can never substitute the examination of the FRAIA, which is precisely the reason why data protection is a necessary but not sufficient attribute of the overall protection of fundamental rights in the context of AI deployment.[168]

Finally, by signing the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law, Ukraine establishes a qualitatively different obligation on the international level, also strengthening the design problem. The Convention demands signatory states to take legislative, administrative, or other actions to enforce human rights responsibilities in the deployment of AI.[169] The White Paper documents Ukraine's commitment to be part of the Council of Europe pilot programme on the development of FRIA methodologies, and institutionalizes the presumption that Ukraine will establish a domestic assessment mechanism.[170] Parkhomenko et al. place this commitment in

---

[164] Kateryna Bodnar, "Regulatory Adaptation of Personal Data Protection Standards to Hybrid Threats in the EU and Ukraine," *Pressing Problems of Public Administration* 2, no. 67 (2025): 426 [in Ukrainian].
[165] Draft Law No. 8153, Arts. 40-41.
[166] Hura, Adaptation to EU AI Act, 124.
[167] Gill-Pedro, Fundamental Rights Impact Assessments, 3-6; Gerards, Schäfer, Muis, and Vankan, FRAIA, 8; Hura, Adaptation to EU AI Act, 126.
[168] Gerards, Schäfer, Muis, and Vankan, FRAIA, 8.
[169] Council of Europe Framework Convention on AI, Arts. 3-5.
[170] White Paper on AI Regulation in Ukraine, 20.

the context of the bigger trend of the Association Agreement implementation in Ukraine, where the legislative approximation in wartime conditions presents a unique challenge and where the obligation to integrate is not postponed.[171] The Framework Convention thereby establishes a normative obligation with no domestic mechanism - a vacuum FRIA is intended to fill. The overlap of the Convention obligation, the approximation requirement of the Association Agreement and the constitutional rights framework forces Ukrainian FRIA-obligation implementation to be a matter of a legal necessity rather than of policy choice.

The pattern of regulation is now, in a sense, systematically unbundled: the idealistic hopes are systematically disengaged with the working legal processes. The provisions of Ukrainian AI-related legislation are fragmentary and not systemic, set out in many regulatory acts that regulate various spheres of public relations.[172] The gap is thus not only a quantitative but qualitative and structural one. Draft Law 8153 addresses the data-protection axis, but there is no instrument available which will address the rest of the aspects that extends between the right to a fair hearing and non-discrimination, dignity, liberty and the full constitutional rights package that Articles 3, 21, 22, and 55 put in place as the content and direction of state activity. The most important aspect is the institutional gap due to the lack of a competent national supervisory authority that can guarantee efficient implementation of future legislations.[173] The FRIA obligation is acknowledged by the own Research Service of the Verkhovna Rada in its analytical note on comparative AI legislation. It states that the impact assessment of fundamental rights is a mandatory part of the deployment and provision of high-risk AI systems.[174] Yukhymenko notes that AI Act high-risk regimes require Member States to designate fundamental-rights authorities, which Ukraine will eventually have to mirror.[175] The gap is thus three-dimensional: an approximation gap, in which no known mechanism meets the FRIA obligation of the EU AI Act against high-risk AI systems in Article 27 and in Annex III; a rights-scope gap, in which the DPIA is focused on data protection but not on the broader fundamental rights portfolio; and a structural quality gap, in which any future mechanism needs to be made to avoid the seven weaknesses previously identified in Article 27 (Section 2.6).

---

[171] Nataliia Parkhomenko, Svitlana Podorozhna, Tetiana Tarakhonych, Stanislav Husarev, and Diana Biloskurska, "Implementation of the Association Agreement with the EU by Adapting Ukrainian Legislation to EU Law," *Social & Legal Studios* 7, no. 1 (2024): 188-189 [in Ukrainian].
[172] Perederii, Legal Principles of AI Use, 55.
[173] Hura, Adaptation to EU AI Act, 125.
[174] Research Service of the Verkhovna Rada of Ukraine, *Analytical Note on Comparative Legislation Regarding the Legal Regulation of Artificial Intelligence Technologies in Ukraine, European States, and the USA* (Kyiv: Verkhovna Rada of Ukraine, 2025), 18-19 [in Ukrainian].
[175] Yukhymenko, AI Regulation Analytical Note, 13.

The design problem, correctly viewed, is an opportunity. Ukraine is not retrofitting a FRIA requirement onto an already established legal framework that is limited by product-safety caselaw, data-protection silos, and a framework that places the fundamental rights below the market integration. It is creating new legislation, well aware of the diagnosed flaws of the EU model, in a constitutional structure that facilitates rights primacy. The National AI Strategy Monograph itself admits that foreign solutions cannot be successfully applied to Ukraine without any introduction, and that Ukrainian specificities require the creation of other developmental trajectories of AI governance.[176]

As a result, Ukraine has a constitutional framework structurally stronger than the treaty-based rights-protective AI governance in the EU, and a series of already existing regulatory tools that individually recognize the issue of AI-mediated rights violations, but which, combined together, form a principle-mechanism gap - principled aspirations systematically disconnected with operative legal mechanisms and leaving a three-dimensional design problem. Sections 3.2 and 3.3 address this three-dimensional design problem through comparative analysis of the Dutch FRAIA, the Canadian Directive on Automated Decision-Making, and the CSDDD, and translate the resulting design lessons into seven legislative and institutional options calibrated to the design corridor the Ukrainian constitutional framework establishes.

### 3.2 Comparative Models and Design Options

This section performs two analytical actions: first, an analysis of three comparative models (the Dutch FRAIA, the Canadian Directive on Automated Decision-Making, and the CSDDD) that reveal possible alternatives to Art 27 baseline design; and second, it uses such comparative results in conjunction with Ukrainian constitutional and policy materials to develop seven possible design options to a Ukrainian FRIA mechanism.

Section 2.6 has determined that Art. 27 has a complex methodological vacuum: it requires a fundamental rights impact assessment but lacks an analytical framework, procedural steps, and participatory structures. The heterogeneity in methodology and rights specification documented in that systematic review confirms that these weaknesses are not unique to Art. 27 but characterize the AI impact-assessment field as a whole.[177] In the case of Ukraine, in a

[176] Shevchenko, ed., Strategy for Artificial Intelligence Development in Ukraine, 80.
[177] Bernd Carsten Stahl et al., "A Systematic Review of Artificial Intelligence Impact Assessments," *Artificial Intelligence Review* 56, no. 11 (2023): 12799, 12812-12815.

situation where legislating is not framed in the logic of internal-market harmonisation in Art. 114 TFEU, three models provide a balanced alternative and outline a design space that is only partially addressed by existing Article 27 of the AI Act. The Dutch "Impact Assessment: Fundamental Rights and Algorithms" (hereafter FRAIA), published by the Dutch Ministry of the Interior and Kingdom Relations in 2022, is the most methodologically complete government-sector FRIA template currently in existence.[178] Its five-part structure - (1) Why (objectives and legal basis), (2A) What: Input (data sources and quality), (2B) What: Throughput (algorithm design and transparency), (3) How (implementation and oversight of output), and (4) Fundamental Rights (the seven-step Fundamental Rights Roadmap) treats rights assessment as a discrete analytical phase rather than a by-product of technical review.[179] The analytical core resides in Part 4's seven-step Fundamental Rights Roadmap: Step 1 identifies the affected rights; Step 2 maps applicable legislation; Step 3 assesses the seriousness of interference through a core-periphery colour-coding system (red for serious interference, yellow for medium-serious one, and green for less-serious interference); Steps 4-7 test the objectives, suitability, necessity, and proportionality of the deployment.[180] The colour-coding system is the FRAIA's key innovation: it adds a qualitative judgment about rights impacts that simple numerical risk scores cannot capture; it reflects the FRAIA's core proportionality logic: the more seriously an algorithm restricts fundamental rights, the more compelling the justification for its deployment must be.[181] This graduated seriousness framework resonates with the Ukrainian National AI Concept's own diagnosis that verifying AI systems' compliance with legislation and existing ethical principles presents a fundamental difficulty - the outlined mechanism provides precisely the structured verification method that the Concept identified as absent.[182]

Continuing, the FRAIA explicitly distinguishes itself from the GDPR Data Protection Impact Assessment, stressing that a DPIA cannot replace a FRAIA, because the former focuses mainly on personal data processing while the latter covers the full range of fundamental rights risks that the colour-coded mechanism exposes.[183] This distinction directly takes into consideration the substitution error that Section 3.1 has identified in Draft Law No. 8153. Additionally, important is the FRAIA multidisciplinary team requirement: legal advisors, data

[178] Gerards et al., FRAIA, 2-4.
[179] Ibid., 5.
[180] Ibid., 67-75.
[181] Ibid., 75.
[182] Concept for the Development of Artificial Intelligence in Ukraine, 3.
[183] Gerards et al., FRAIA, 8.

scientists, domain experts, and communication specialists form the mandatory multidisciplinary team, with citizen panel representatives and interest group representatives recommended as desirable participants where possible - including from the earliest Part 1 stage of objective definition.[184] The fact that the citizen panel representation is introduced at the stage of the objective definition proves that efficient involvement in FRIA processes is not a dream, but a reality. The major weakness of the FRAIA is, however, the fact that it is voluntary: it is a commitment of the government and not a legal obligation. In the case of Ukraine, this is not a disqualifying restriction but an enabling point - the Dutch model illustrates what a binding FRIA approach might resemble, and Ukraine will have to make a decision about whether to codify the substantive content.

The Canadian Directive on Automated Decision-Making, introduced through the Treasury Board of Canada Secretariat in 2019 and last amended in 2025, is so far the most sophisticated compulsory impact evaluation framework for AI deployment.[185] Its system of four levels categorizes automated decision-making systems based on a composite evaluation of rights, dignity, privacy, autonomy, health, and economic effects, with a scale to the severity, reversibility, and duration of each effect.[186] Level I systems (low impact, easily reversible consequences) have few obligations, whereas Level IV systems (very high impact, irreversible consequences) demand consent of Treasury Board before deployment can proceed. This is a true graduated proportionality system - a spectrum model where obligations increase linearly with risk. The Canadian emphasis on the decision process, as opposed to the type of technology, allows the instrument to be technically neutral, and yet, normatively accurate.[187]

Canadian Directive has three attributes which are analytically relevant in relation to Art. 27 baseline. First, its pre-production mandatory publication norm, that requires federal institutions to post the results of Algorithms Impact Assessment on the Open Government Portal prior to deployment, has the effect of transparency allowing civil society to review the findings before it is too late.[188] Second, its graduated human involvement requirements indicate that Level III and IV systems must have the final decision been made by a human. This operationalises Art. 14 of the human oversight principle of the EU AI Act in tangible, practical,

---

[184] Ibid., 2-3, 10.
[185] "Directive on Automated Decision-Making," Treasury Board of Canada Secretariat, Ottawa, 2019, amended 2025, §1.
[186] Ibid., Appendix B.
[187] Jakob Mökander, Jonas Schuett, Hannah Rose Kirk, and Luciano Floridi, "Auditing Large Language Models: A Three-Layered Approach," *AI and Ethics* 4, no. 4 (2024): 1090-1095.
[188] Directive on Automated Decision-Making, §6.1.1.

actionable language that is absent in Art. 27.[189] Third, the Directive bases testing responsibilities on named legal instruments - the Canadian Charter of Rights and Freedoms, the Canadian Human Rights Act, and the United Nations Declaration on the Rights of Indigenous Peoples Act, thus anchoring it to a set of statutory tools, and establishing a reviewable standard of legal violation instead of leaving the rights assessment to the unfettered whim of the deployer.[190]

It should be noted that the Canadian model was mentioned in a staff working document by the Commission that accompanied the proposal of AI Act, where it was expressly rejected based on the harmonization considerations that are not part of rights protection.[191] This institutional decision was, in turn, an indication of the market-integration logic that limited the design of the FRIA under Art. 114 TFEU. Since Ukraine is a candidate state that is legislating under its own constitutional framework it is free to refer to the Canadian model. Ukraine's adaptation imperative has a dual nature, both the legal necessity to harmonize with the acquis and the economic necessity of orienting the IT sector toward the EU market, but neither dimension requires Ukraine to reproduce the limitations that the EU's own harmonization constraints imposed on Art. 27.[192]

The Corporate Sustainability Due Diligence Directive (Directive 2024/1760, hereafter CSDDD) adds the last component to the comparative triangulation in terms of giving a structural argument concerning the logic of EU legislation per se. The CSDDD requires mandatory human rights compliance with mandatory stakeholder participation on five stages through which rights protection, as opposed to product safety or market harmonisation, is the main legislative objective.[193] Article 13 entails that companies should conduct meaningful engagement whenever there is an identification, assessment, cessation, remediation, and monitoring of the affected stakeholders while Article 3(n) has a very broad definition of stakeholders which includes affected communities, workers, trade unions, and civil society organizations.[194] The six-step due diligence process set out in Recital 20 ((1) integrating due diligence into policies and management systems, (2) identifying and assessing adverse impacts,

---

[189] Ibid., Appendix C.
[190] Ibid., §6.3.3.
[191] "Commission Staff Working Document: Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," European Commission, SWD(2021) 84 final, Brussels, 21 April 2021, 58.
[192] Hura, Adaptation to EU AI Act, 120.
[193] CSDDD, Art. 13(1)-(3).
[194] Ibid., Arts. 13(1)-(3), 3(n).

(3) preventing, ceasing or minimizing those impacts, (4) monitoring and assessing the effectiveness of measures, (5) communicating, and (6) providing remediation) provides a procedural template that maps onto Mantelero's three-phase FRIA framework: steps one and two correspond to planning and scoping, steps three and four to risk analysis and management, and steps five and six to the communication and remediation outputs.[195]

The CSDDD argument is not that it is directly applicable to AI governance (it is not) but that it disproves that compulsory stakeholder involvement as structurally incompatible with the EU approximation. Art. 27 of the EU AI Act contains no participation requirement, as Section 2.6 identified. The CSDDD shows that this lack is not normative but conditional: it is the result of the product-safety legal underpinning of the AI Act and of trilogue politics, rather than some dedication to not involve rights-assessment instruments. The content of EU fundamental rights protection often follows a kind of economic rationality - where that rationality is that which organizes the legislative tool, participation is optional and where rights protection is central, it is compulsory.[196] The National AI Concept itself states that the key task of the state policy in the sphere of legal regulation of the AI industry is to provide the protection of the rights and freedoms of the relations participants within this industry. This makes the protection of rights, as opposed to market facilitation, the main aim of legislation and thus makes the legislative design in Ukraine geared towards the rights-centric logic of the CSDDD as opposed to the product-safety logic of the AI Act.[197] Legislating with this rights primacy as a mandatory constitutional rule under Article 3, Ukraine can and should make stakeholder participation binding.

The three comparative models collectively establish four design principles that inform the options developed below. First, from the FRAIA: a structured, staged methodology with colour-coded graduated severity is both feasible and operational - and directly addresses methodological vacuum and product-safety mismatch identified in Section 2.6. Second, from the Canadian Directive: statutory rights anchoring, mandatory publication, and graduated obligations calibrated to impact severity are achievable within a binding legal framework - addressing scope limitation and enforcement deficit. Third, from the CSDDD: mandatory stakeholder participation is structurally compatible with the EU acquis and directly addresses participatory deficit. Fourth, taken together, all three models demonstrate that the right-centric,

[195] Ibid., Recital 20.
[196] Augenstein, Engaging the Fundamentals, 1917.
[197] Concept for the Development of Artificial Intelligence in Ukraine, 10.

participatory, and methodologically rigorous FRIA that Article 27 fails to deliver is not an idealist construction but a regulatory reality in comparable jurisdictions - a comparative fact that, as established in Section 3.1, Ukraine is constitutionally positioned and legally obligated to replicate.

The comparative analysis confirms that there are alternatives to the design options of Art. 27, which have been legislated and are based on consistent regulatory theory. Seven of the design options listed below will deal with one or more of seven weaknesses (identified in Section 2.6), based on above comparative models and on Ukrainian sources (in particular the Monograph and the government own policy documents).

**Design Option 1 - Constitutional Anchoring**

The first design option concerns the constitutional anchoring of Ukraine's FRIA-type obligation. Art. 27 has a product-safety mismatch that hierarchically subordinates the protection of rights with a market-integrity logic. Ukraine legislation thus must indicate explicitly, in its provision of purpose, that the FRIA obligation is adopted to discharge the positive obligation, which is stipulated under Article 3 of the Constitution of Ukraine and states that the content and orientation of the state activity are determined with references to the rights and freedoms of the person.[198] This clause forms the interpretive canon: where there is ambiguity, the interpretation that maximises protection of rights is enforced by the non-regression guarantee of Article 22 of the Constitution[199] - this determines the instrument's interpretive frame and its position in the hierarchy of legal norms. Shevchenko et al. state in the final provisions of the national AI Strategy, that the Strategy is grounded on the Constitution of Ukraine.

Additionally, the Strategy itself mandates that AI governance mechanisms record the ethical, legal, and social consequences of AI deployment.[200] Constitutional mandate is therefore already translated into the AI governance terms, the only thing lacking is the process by which it is put into action. Dworkin's 'rights as trumps' theory makes the constitutional principle an operational rule of FRIA: the question should be whether an AI system deprives individuals of rights and not whether the they generate net social benefits in general.[201] Parkhomenko et al. reinforced this by explaining European integration as a civilisational choice entrenched in

[198] Constitution of Ukraine, Art. 3.
[199] Ibid., Arts. 21-22.
[200] Shevchenko, ed., Strategy for Artificial Intelligence Development in Ukraine, 84, 96.
[201] Bowie, Review of Taking Rights Seriously, 908, 912.

Ukrainian Constitution meaning that the duty to approximate EU law and the duty prioritise constitutional rights do not conflict with each other but reinforce, since approximation must be fulfilled in a rights-first manner.[202]

**Design Option 2 - Universal Deployer Coverage**

The second design option relates to the area of deployer coverage. EU AI Act limits the FRIA obligation to a specific sub-group of deployers, namely, public bodies, public-service providers, and some financial-sector actors. The potential Ukraine's FRIA mechanism needs to apply to all high-risk AI system deployers, as a personal employment-screening algorithm that discriminates against internally displaced individuals presents the same fundamental rights risks regardless of whether the deployer is a state or a private entity. The Art. 27(1) restriction is a product of EU trilogue compromise, not principled rights reasoning. The expansion to universal coverage should, however, be accompanied with progressive requirements that are also adjusted to the extent of rights violation. The grading process of such violation, for instance, can be based on the colour-coding model of the Dutch FRAIA: green (peripheral interference) imposes standard documentation requirements; yellow (medium-serious interference) imposes due diligence and supervisory notification; red (core interference) imposes pre-deployment supervisory consultation and human review, similar to the Level III and IV requirements of the Canadian Directive.[203]

**Design Option 3 - Prescribed Three-Stage Methodology**

The third design option addresses the recommended methodology. Under Art. 27 FRIA is required without mentioning any analytical approach, leaving deployers to decide on what method to use for the assessment. Ukraine's legislative instrument should require three-stage approach: context mapping (system description, affected-population identification and rights inventory), impact assessment (severity assessment with the help of core-periphery framework, analysis of intersectionality, and scenario modelling), and mitigation with monitoring (specification of measures, review triggers and documentation standards). The White Paper itself identifies the development or adaptation of a methodology for assessing AI's impact on human rights as a key tool for both future national regulation and EU market access.[204] This design option hence operationalises the policy intention of the government itself as opposed to

[202] Parkhomenko et al., Implementation of the Association Agreement, 185.
[203] Gerards et al., FRAIA, 75; Directive on Automated Decision-Making, Appendix B.
[204] White Paper on AI Regulation in Ukraine, 19-20.

imposing an externally derived obligation. Recent methodological innovations in the literature should also be treated as binding design requirements: structured, rights-by-rights assessment tools that operationalize Charter rights through detailed questionnaires and scoring matrices to enable comparability across assessments, and the scenario-based approach to risk presented by Novelli and colleagues that conceptualizes risk as a variable of hazard, exposure, vulnerability, and capacity to respond, allowing distributional impact analysis of the different segments of the population in the context of various deployment scenarios - an analytical capability especially useful to the displaced populations in Ukraine and the socioeconomic stratification in war.[205]

**Design Option 4 - Mandatory Stakeholder Participation**

This option responds directly to participatory deficit identified in Section 2.6: the absence of any mandatory obligation to consult rights-holders is the structural feature of Article 27 most inconsistent with the HRIA tradition, and it is the design gap most clearly addressable by reference to the CSDDD participatory architecture.

The fourth design option is related to the compulsory involvement of the stakeholders. Ukraine should implement three levels of participation that will be adjusted to the severity of the rights violation, possibly under the FRAIA color-grade assessment. At the disclosure level (green), deployers post a FRIA summary, which allows civil society to review it, but does not impose on less risky systems the same burdens of consultation. At the consultation level (yellow), deployers give draft FRIA results to representatives of the affected communities to comment in writing on before the finalisation, with a requirement of written comment to substantive submissions. At full participation (red, core interference) the structured involvement of rights-holders (including organizations representing vulnerable groups) is required before the impact evaluation stage, as per CSDDD Article 13(3)(a) pattern.[206] The National Council on AI Safety, suggested in the Monograph by Bilokobylskyi, has a clear role of collaboration with European and international AI regulation agencies, and interaction with civil society - institutional architecture that assumes organized involvement as opposed to viewing it as a voluntary addition to a technocratic evaluation procedure.[207] International

[205] Claudio Novelli, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo, and Luciano Floridi, "AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act," *Digital Society* 3, no. 1 (2024): 3-5.
[206] CSDDD, Art. 13(3)(a).
[207] Oleksandr V. Bilokobylskyi, "To Section 3 'Aims and Objectives of the Strategy' and Section 6 'AI Governance System,'" in Strategy for Artificial Intelligence Development in Ukraine: Monograph, ed. Anatolii I. Shevchenko (Kyiv: Institute of Artificial Intelligence Problems of the MES and NAS of Ukraine, 2023), 97-102.

human rights law further demands substantial consideration of those who are affected by any assessment of the protection of their rights, and thus participation is not a procedural nicety but an essential part of the rights framework itself.[208]

**Design Option 5 - Rights-Competent Supervision**

The fifth design option concerns rights-competent supervision. Because the EU's market surveillance authorities are institutionally structured for product-safety rather than rights supervision, Ukraine should not replicate that template. Instead it should adopt a hybrid framework in which fundamental rights are again put as primary purpose of AI governance architecture: the national data protection authority should become the competent body in the core, and its mandate would explicitly be extended beyond data protection to include AI-specific fundamental rights oversight; an expert AI advisory board should provide cross-disciplinary human-rights and technical experience that market surveillance bodies usually do not have; and sector-specific consultation processes in areas like healthcare, policing, and social protection would guarantee context-sensitive analysis of potentially risky deployments that a generic product-safety regulator could not offer.

This is where the contribution of the Monograph in terms of the institutional design may be useful. The suggested National Council on AI Safety model includes pre-deployment assessment and lifecycle monitoring, EU-standards compliance verification, and international cooperation capabilities, precisely the blueprint of the advisory council element.[209] Moreover, it must be noted that the lack of an independent data protection body with equivalent powers to those of the European counterparts is one of the constant complaints European Commission has of the progress of the Ukrainian integration into the EU, and the establishment of a rights-competent supervisory organization is thus becoming not only a domestic governance enhancement but an accession precondition.[210] In this regard, by establishing a rights-competent supervisory ecosystem with an empowered data protection authority and a specialized AI advisory council, Ukraine would not only be able to meet EU accession standards, but will also entrench fundamental rights as the organizing principle of its new AI governance order.

**Design Option 6 - Mandatory Enforcement**

---

[208] Lorna McGregor, Daragh Murray, and Vivian Ng, "International Human Rights Law as a Framework for Algorithmic Accountability," *International and Comparative Law Quarterly* 68, no. 2 (2019): 309-311.
[209] Bilokobylskyi, To Section 3 and Section 6, 97-102.
[210] Bodnar, Regulatory Adaptation of Personal Data Protection Standards, 428.

The sixth design option addresses mandatory enforcement. EU AI Act's enforcement architecture relies on the general penalty provisions without specifying FRIA-specific sanctions meaning at least three interlocking enforcement components are required. To begin with, administrative penalties against non-compliance with FRIA should be established on the highest level of the Ukrainian AI regulation system. Second, there should be a pre-deployment consultation trigger similar to GDPR Article 36 where the FRIA discloses unmitigated high-risk interference with core rights: the deployer should consult the supervisory authority prior to deployment while the deployment compliance with this requirement would constitutes a higher-tier violation. Third, any impacted individual should possess a legally binding right to access the FRIA carried out regarding any AI system whose output has a significant influence on their rights.

Furthermore, Ukraine's formalised participation in the European AI Board, achieved in October 2025, is an additional reason to believe a binding enforcement is justified - being a part of the coordination organ in charge of FRIA enforcement across the EU establishes an institutional expectation that the Ukrainian enforcement system will be equally strong.[211] At the same time the middle government readiness scores (according to the Monograph data) and infrastructure gaps in Ukraine imply that enforcement mechanisms should be implemented in phases in line with the institutional capacity-building since the imposition of the highest-tier penalties without the necessary institutional support would be counterproductive.[212]

**Design Option 7 - Integrated FRIA-DPIA Architecture**

The seventh design option is the integrated FRIA-DPIA architecture. As was previously established, the coexistence of GDPR DPIA requirements and the FRIA of the AI Act creates assessments fragmentation. The fact that Ukraine is basically simultaneously drafting both Draft Law No. 8153 on personal data protection and the AI governance framework gives it a chance, not available to any EU Member State: the two instruments could be designed as an integrated assessment architecture. Bodnar identifies Draft Law No. 8153 as the key legislative instrument for introducing a DPIA procedure in cases of high-risk processing,[213] which suggests that this framework could also be used as a foundation for developing a future FRIA regime in Ukraine. The sequential arrangement works in the following way: the DPIA under

[211] Yukhymenko, AI Regulation Analytical Note, 3.
[212] Yuriy P. Kondratenko, Oleksiy S. Striuk, Oleksii V. Kozlov, and Ievgen V. Sidenko, "To Section 1 'Paradigm,'" in Strategy for Artificial Intelligence Development in Ukraine: Monograph, ed. Anatolii I. Shevchenko (Kyiv: Institute of Artificial Intelligence Problems of the MES and NAS of Ukraine, 2023), 126-148.
[213] Bodnar, Regulatory Adaptation of Personal Data Protection Standards, 426.

Draft Law No. 8153 will be filled in the first place, providing a data-flow map, an analysis of affected persons, and a preliminary rights inventory in accordance with the Articles 39 to 41.[214]

The FRIA will then apply the analysis to the rights beyond data protection - such as non-discrimination, due process, freedom of expression, the right to an effective remedy, collective and group effects, intersectionality, and, for instance, the full FRAIA proportionality test. The FRIA report will refer to and catalogue the DPIA findings, and capture the rest of the rights risks falling out of the data protection frame. The Dutch FRAIA has explicitly stated that a DPIA cannot replace the larger-scale FRAIA review, creating the principle of separation, and the sequential model suggested here imposes this principle operationally without the duplication of assessment effort.[215] Positioning the FRIA as the more general instrument, where DPIA will be a sufficient component, establishes the protection of rights, as the visual and procedural superstructure where the data protection will be one of the core elements. Institutionally, this kind of integrated chain would enable Ukraine to escape the duplicative siloed processes which define the present EU space and instead operationalize a unitary coherent *ex ante* process where data protection and more fundamental rights protection safeguards are mutually reinforcing as opposed to competing compliance checklists.

In conclusion, the comparative analysis and seven design choices show that a FRIA mechanism for Ukraine is not a utopian construction: it can be constitutionally anchored in the rights-primary framework, methodologically grounded in models like Dutch FRAIA and the Monograph's social-threat taxonomy, participatory in the sense required by the CSDDD and the Council of Europe Framework Convention pilot, while being supervised by a rights-competent hybrid authority modelled on the National Council proposal and domestic bioethics committees, enforced through binding sanctions calibrated to institutional capacity, and integrated with the DPIA via a sequential architecture of Draft Law No. 8153 and the new AI governance framework. These seven options are not independent enhancements, but mutually supporting architecture: constitutional anchoring makes the scope extension possible; universal scope requires a prescribed methodology; methodology needs supervision; supervision demands enforcement; and integrated design prevents the whole architecture from being vulnerable to evasion.

---

[214] Draft Law No. 8153, Arts. 39-41.
[215] Gerards et al., FRAIA, 8.

### 3.3 Potential Institutional Architecture

The identified institutional vacuum in Ukrainian AI regulation is not simply a lack of capacity but a structural flaw that negatively affects the whole regulatory framework suggested in this chapter. As Hura concludes - institutional challenge is the most critical due to the absence of a competent national supervisory authority capable of ensuring effective enforcement of future legislation.[216] Without such authority, a potential FRIA methodology becomes a documentation exercise and constitutional anchoring of fundamental rights assessment remains aspirational rhetoric rather than enforceable obligation. The institutional question is thus not peripheral to the FRIA design - it is the condition, on which all the other design decisions will be based.

The institutional framework proposed in this section operationalizes Design Option 5 (rights-competent supervision) and Design Option 6 (mandatory enforcement) from Section 3.2 by translating their requirements into a concrete phased architecture calibrated to Ukraine's current institutional capacity. The Monograph provides the most operationally developed institutional template to fill this gap. Bilokobylskyi suggests a National Council on AI Safety under the Prime Minister with four specified functions which exactly correlate with the FRIA institutional needs: first, the initial review of high-risk AI systems on whether they comply with the principles and ethical norms - the FRIA pre-deployment review role; second, periodic review of adopted high-risk AI systems during the lifecycle to examine the effects of AI systems on society - the iterative role; third, verification of compliance with European standards of security, data protection and privacy - the function of approximation verification; and fourth, collaboration with European and international regulators of AI - the institutional connection with the European AI Board.[217]

This fourth function gained tangible importance when Ukraine became a member of the European AI Board in October 2025 and established a direct institutionalized channel of supervisory coordination through which the proposed National Council would provide specific operationalization on the domestic level. The National Council would not substitute the potential data protection authority but would complement it as a specialized advisory-to-regulatory body on the fundamental rights aspect of AI regulation.

It should be also noted that the proposed Council is not an unprecedented innovation.

---

[216] Hura, Adaptation to EU AI Act, 125.
[217] Bilokobylskyi, To Section 3 and Section 6, 97-102.

Chebanov, in the Monograph, finds the Committee on Bioethics under the Cabinet of Ministers (active since 2001) as an analogous institutional model.[218] Bioethics committees fulfill the role of ethical expertise of new medical technologies, the effects of which create complex moral issues that are beyond the capacity of traditional expert institutions to address - a structural analogy to the role a FRIA-administering institution should play with emerging AI technologies. Ukraine signed the Council of Europe Convention on Human Rights and Biomedicine (Oviedo Convention, ETS-164) in 2002, establishing a political commitment to rights-protective technology governance that has been reflected in domestic bioethics regulation - even though formal ratification has not yet occurred and the Convention therefore does not create binding treaty obligations.[219] By functional analogy, this commitment to rights-protective oversight of new technologies extends to the AI governance context. Separately, Ukraine's signature of the Council of Europe Framework Convention on Artificial Intelligence (CAIF) creates the binding international obligation to establish rights-protective AI oversight mechanisms, as established in Section 3.1. Chebanov applies the four classical principles of bioethics, such as autonomy, non-maleficence, beneficence, and justice, to the governance of AI, and shows that the analytical model of autonomous expert ethical judgment has already been institutionalized in Ukrainian legislation.[220] The proposed AI rights advisory council might be directly based on this template: it must be multidisciplinary, independent, advisory-to-regulatory in operation, and under the oversight of the Cabinet of Ministers.

However, the suitability of the institutional ambitions has to be adjusted to the operational reality. The data in the Monograph on AI Readiness Index suggests the proportionality argument of the institutional development phase: the score of 41.88 out of 100 of AI Readiness in Ukraine, with the governmental readiness of 41 out of 100 and infrastructure at 30.3 out of 100, shows that the immediate institutional deployment cannot be made.[221]

A staged implementation plan is therefore the right option. At Phase 1, which can start immediately under the current law and potential adoption of Draft Law No. 8153 and corresponds to Stage 1 of the White Paper, the data protection authority would use its oversight

---

[218] Viktor B. Chebanov, "To Subsection 7.3 of Section 7 'Artificial Intelligence in Medicine,'" in Strategy for Artificial Intelligence Development in Ukraine: Monograph, ed. Anatolii I. Shevchenko (Kyiv: Institute of Artificial Intelligence Problems of the MES and NAS of Ukraine, 2023), 239-242.
[219] 'Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (Oviedo Convention),' Council of Europe, European Treaty Series No. 164, 4 April 1997.
[220] Chebanov, To Subsection 7.3, 240-241.
[221] Kondratenko et al., "To Section 1 'Paradigm,'" 138.

powers to review FRIA questions alongside the DPIA, relying on the prior-consultation procedure already set out in Draft.[222] At Phase 2, once hostilities have ended and dedicated AI legislation has been enacted, the National AI Safety Council will be instituted as a specialized agency with FRIA pre-deployment inspection authority, based on Bilokobylskyi design template. Finally, at Phase 3, during the pre-accession alignment phase, the supervisory architecture of Ukraine will become part of the coordination structure of the European AI Board, providing the institutional connection with EU.[223]

With that said, the only way that a phased roadmap would be credible is when it is anchored in an institution that can take this role from the outset. This data protection authority may be the natural lead competent authority in the first phase and its role must be considered not as a one-off expedient but as a permanent part of the hybrid supervisory architecture. Article 40 of Draft Law 8153 already imposes a deployers requirement to consult with the supervisory authority in respect of the processing which raises high risks to rights and freedoms - a structurally equivalent mechanism to FRIA pre-deployment review.[224]

The best institutional architecture for Ukraine to adopt is a hybrid one: the data protection authority as the lead competent authority with an expanded mandate, supplemented by a National AI Safety Council. The staged process of implementation ensures that institutional ambition is grounded in operational viability. This architecture is designed not for perfect conditions, but to work within the constraints that wartime imposes as it builds the institutional infrastructure that post-conflict reconstruction will need.

### 3.4 Conclusions of Chapter III

Chapter III establishes that Ukraine's position as a late adopter of AI governance constitutes a design opportunity rather than a limitation. Three overlapping factors enable this: first, a constitutional framework under Articles 3 and 22 of the Constitution of Ukraine that structurally requires rights primacy and prohibits regression; second, the simultaneity of Draft Law No. 8153 and the emerging AI legislation, which permits integrated design rather than retroactive coordination; and third, the approximation obligation under Article 474 of the Association Agreement, which demands functional equivalence with the rights-protective objectives of the EU model rather than verbatim reproduction of its institutional

[222] White Paper on AI Regulation in Ukraine, 12, 18-19; Draft Law No. 8153, Art. 40.
[223] Hura, Adaptation to EU AI Act, 125.
[224] Draft Law No. 8153, Art. 40.

compromises.[225] Together, these factors mean that a Ukrainian FRIA mechanism that addresses the seven structural weaknesses identified in Chapter II is not merely permissible within the approximation framework - it is the form of transposition most faithful to the stated purpose of Article 1 of the AI Act itself.

The seven design options developed in Sections 3.2 and 3.3 form an interdependent architectural system rather than a menu of independent enhancements. Constitutional anchoring enables universal deployer coverage; universal coverage requires a prescribed three-stage methodology; methodology requires participation; participation requires rights-competent supervision; supervision requires binding enforcement with a prior-consultation trigger; and integrated FRIA-DPIA architecture prevents the assessment fragmentation that would otherwise disperse enforcement capacity. Partial implementation of this system is structurally counterproductive: each component relies on the others to produce its rights-protective effect.

Four real constraints must be built into the implementation strategy. The wartime institutional context limits the pace of Phase 1 deployment. The principle-mechanism gap cannot be eliminated by legislative design alone. The absence of empirical validation of the seven options means the proposal remains normative rather than evidence-based. And the post-Soviet administrative culture of compliance-as-formality poses a political-economy risk that statutory language alone cannot resolve. These constraints are not qualifications that undermine the design options; they are the reasons why the options are designed as they are - with constitutional anchoring that survives operational pressure, prescribed methodology that makes compliance measurable, participatory mechanisms that provide accountability independent of state capacity, and enforcement provisions that convert rights protection from an aspiration into a concrete constraint on deployment decisions.

The structural weaknesses of Article 27 identified in Chapter II are not unavoidable features of rights-protective AI regulation; they are consequences of the EU's internal-market constitutional structure - a structure Ukraine need not and should not reproduce. The overall Conclusions and Recommendations translate these findings into specific propositions addressed to Ukrainian legislators, the supervisory authority, and the scholarly community.

[225] EU-Ukraine Association Agreement, Art. 474.

## CONCLUSIONS

The FRIA under Article 27 of the EU AI Act in its current form is structurally predisposed to function as a formalistic compliance mechanism rather than a genuine *ex ante* fundamental rights protection instrument. This determination is not incidental to the instrument's design - it is structurally embedded in the choice of Article 114 TFEU as legal basis and the New Legislative Framework as regulatory model, which together configure rights protection as a secondary constraint on market integration rather than as the instrument's primary mandate. The six conclusions below set out the analysis supporting this determination, organised in line with the three research objectives, with each objective addressed through two numbered points:

**Objective 1 - Normative criteria (Chapter I)**

1. The conceptual and normative foundations of the FRIA are determined not by Article 27 but by the interaction of three structural factors reconstructed in Chapter I. First, high-risk AI deployment engages a broad and context-dependent range of Charter rights whose impact varies with the deployment setting and cannot be captured by a pre-market technical evaluation alone. Second, the structural limitation of the FRIA does not arise from Article 114 TFEU as a legal basis: the GDPR, adopted on the same legal basis, demonstrates that internal-market competence is capable of generating substantive rights protection. The limitation arises instead from the regulatory model the legislator chose to build on that basis: the New Legislative Framework product-safety architecture allocates the fully harmonized obligations to the provider, while the deployer bearing the Article 27 FRIA obligation operates under a qualitatively different logic that, on Gill-Pedro's teleological analysis, functions as a minimum standard Member States may exceed, leaving the deployer simultaneously dependent on provider-stage information. Article 1's rights protection objective therefore functions as a secondary consideration within an instrument whose primary telos is market integration. Third, Ukraine's position is qualitatively distinct from the classical Brussels Effect: approximation under the Association Agreement is a legal obligation of convergence, not a competitive incentive, which means the structural limitations of Article 27 are transmitted by legal requirement rather than by voluntary adoption.

2. The normative criteria against which Article 27 must be assessed are not derived from the AI Act itself but from the impact-assessment tradition, in particular the DPIA under Article 35 GDPR, the HRIA methodology in the UN Guiding Principles on Business and Human

Rights, and the frameworks of Mantelero and Götzmann. A methodologically adequate impact assessment is (1) informed by international human rights standards, not limited to domestic compliance; (2) participatory in its engagement with affected rights-holders; (3) sensitive to equality and intersectional harm; (4) transparent and accountable in its methodology and conclusions; and (5) iterative rather than a one-off pre-deployment formality. These criteria constitute the yardstick against which the substantive performance of Article 27 is measured in Chapter II and against which the Ukrainian design is constructed in Chapter III.

**Objective 2 - Structural diagnosis of Article 27 (Chapter II)**

**3.** The legal nature, scope, methodology, institutional architecture and enforcement of Article 27 suffer from seven mutually reinforcing structural weaknesses that are not separate drafting errors but joint consequences of inserting a rights-protection function into an internal-market instrument (Section 2.6): (a) a product-safety mismatch, by which the deployer's risk identification under Article 27(1)(d) is structurally dependent on provider information under Article 13 - an information asymmetry the reliance mechanism of Article 27(2) only partially mitigates; (b) a scope limitation confining the obligation to public-law bodies, public-service providers, and Annex III(5)(b)/(c) deployers while leaving structurally equivalent private-sector deployments outside; (c) a methodological vacuum, since Article 27(5) prescribes a documentary template but not an analytical method; (d) an institutional misfit, because the market surveillance authorities of Article 27(3) are equipped for product-safety, not rights, oversight and because Article 27(4) does not resolve MSA-DPA jurisdictional overlap; (e) an enforcement deficit, Article 27 being absent from the Article 99(4) penalty schedule and lacking an Article 36-GDPR-type prior-consultation trigger; (f) assessment fragmentation across FRIA, DPIA and HRIA that Article 27(4)'s complementarity formula does not cure; and (g) a participatory deficit, where Article 27 is imposing no obligation to consult, engage, or obtain input from affected rights-holders at any stage of the assessment process - a structural departure from the HRIA criterion of participation as established in Section 2.2 and confirmed by the criterion-by-criterion test in Section 2.5 - that reduces the FRIA to an internal documentation exercise conducted by the deployer without the involvement of those whose rights are at stake.

**4.** The comparative analysis of FRIA against HRIA and DPIA conducted in Section 2.5 establishes that Article 27 fails to satisfy any of the four process criteria (participation, non-discrimination, empowerment, and accountability - encompassing transparency and

access to remedy) as binding legal requirements: where Article 27 makes contact with these criteria at all, it does so in fragmentary and non-enforceable form (the Article 86 right to explanation as a partial empowerment fragment; documentation and MSA notification as a partial accountability fragment), in each case falling short of the binding requirement that the HRIA tradition demands. Against the content criteria (use of international human rights benchmarks, comprehensive scope of impacts, severity assessment including scope, extent and irremediability, the avoid-reduce-restore-remediate mitigation hierarchy, and access to remedy) Article 27 performs only partially. The "check-box exercise" risk is therefore not an implementation concern but a structural property of the instrument: the questionnaire template of Article 27(5), the absence of substantive penalties in Article 99(4) and the lack of a mandatory stakeholder participation obligation jointly secure the form of rights assessment without its substance.

**Objective 3 - Ukrainian legislative design (Chapter III)**

**5.** The approximation obligation of Ukraine under Article 474 of the Association Agreement and the accession acquis is a result-oriented duty of functional equivalence rather than a demand for verbatim legislative imitation. Ukraine's constitutional framework together with the simultaneity of Draft Law No. 8153 and the emerging AI legislation not only permits but normatively requires a FRIA design that corrects the seven weaknesses of Article 27 rather than reproducing them. The Brussels Side-Effect identified in Section 1.3 reinforces this conclusion negatively: a verbatim transposition would lock Ukraine into the structural deficiencies diagnosed in Chapter II without any countervailing rights-protective gain, exporting to the Ukrainian legal order the very pathologies that approximation is meant to remedy. A constitutionally anchored, methodologically prescribed, participatory and enforceable Ukrainian FRIA is therefore more compliant with the rights-protective objective of Article 1 of the AI Act than a verbatim transposition of Article 27 would be.

**6.** The seven design options developed in Section 3.2 and operationalized in Section 3.3 form an interdependent system rather than a set of optional improvements: constitutional anchoring enables universal scope; universal scope requires prescribed methodology; methodology requires rights-competent supervision; supervision requires binding enforcement; and integrated architecture prevents assessment fragmentation. Partial implementation is structurally counterproductive. Four factual constraints must be built into the implementation strategy but these constraints are reasons to institutionalize normative ambition rather than to dilute it.

## RECOMMENDATIONS

The following recommendations are addressed to the Ukrainian legislator and to the supervisory authorities responsible for AI governance, in line with Conclusions 5 and 6.

1. To adopt a Law of Ukraine on Artificial Intelligence, or another comprehensive legislative act regulating artificial intelligence, which includes a dedicated provision on the Fundamental Rights Impact Assessment for high-risk AI systems. The purpose clause of that act should expressly ground the FRIA obligation in Article 3 of the Constitution of Ukraine and, by virtue of the non-regression guarantee of Article 22, require a rights-maximizing interpretation in cases of ambiguity. This is the necessary legislative vehicle for introducing a coherent Ukrainian FRIA mechanism.
2. To extend the personal scope of the obligation to all deployers of high-risk AI systems irrespective of public or private status, with graduated procedural requirements calibrated to severity: green (peripheral interference, standard documentation), yellow (serious interference, supervisory notification and due diligence), and red (core interference, mandatory prior supervisory consultation and human review). This implements design options 2 and 4 and cures the scope limitation and participation gap identified in Article 27 AI Act.
3. To amend Articles 39-41 of Draft Law No. 8153 to establish a sequential FRIA-DPIA architecture: the DPIA component is governed by those articles and Article 40's prior-consultation duty bridges to the FRIA, while the future AI law or comprehensive AI regulatory act governs the rights assessment beyond data protection. This operationalizes design option 7 and cures fragmentation without duplicative documentation.
4. To establish the hybrid supervisory architecture of design option 5 in two steps. First, the mandate of the future national data protection authority should be expanded, through amendment to Articles 39-41 of Draft Law No. 8153, to include AI-related fundamental rights oversight and to serve as the lead competent authority in Phase I. Second, a National Council on AI Safety should be established by Resolution of the Cabinet of Ministers of Ukraine, on the institutional template of the Committee on Bioethics, with the four functions identified in Section 3.3: pre-deployment review, lifecycle monitoring, European-standards verification, and coordination with the European AI Board.
5. To prescribe in the future AI law or comprehensive AI regulatory act a mandatory FRIA

methodology based on the HRIA tradition rather than on a simplified questionnaire model. At minimum, the law should require scoping of the deployment context, identification of affected rights and groups, assessment of severity and likelihood of harm, formulation of mitigation measures, reasoned deployment decision, and periodic review where the system, context, or risk profile materially changes.

6. To require meaningful stakeholder participation wherever deployment of a high-risk AI system is likely to affect identifiable individuals or groups. Where direct consultation is not possible, the deployer should be required to justify that impossibility in writing and to adopt equivalent participatory safeguards, including consultation with civil society organizations, professional associations, or affected-group representatives.
7. To impose on every provider of a high-risk AI system placed on the Ukrainian market a legal duty to supply deployers with the documentation necessary for a genuine deployment-stage rights assessment, including intended purpose, known limitations, performance conditions, foreseeable misuse, the rights-relevant outputs of the provider's own pre-market evaluation, and relevant risk-management information. The duty should be calibrated to Article 13 of the EU AI Act so that a provider already discharging the equivalent EU duty is presumptively compliant under Ukrainian law, and should be enforceable through the same supervisory and sanctions regime that applies to the deployer's FRIA obligation. This recommendation corrects the structural information asymmetry between provider and deployer identified in Chapter II without imposing duplicative obligations on providers already subject to the AI Act.
8. To provide in Ukrainian legislation that failure to conduct a FRIA, serious methodological defects in its preparation, failure to implement mandatory mitigation measures, or deployment in breach of a prior-consultation duty shall constitute separate offences subject to effective, proportionate, and dissuasive sanctions. Without such enforcement rules, the Ukrainian model would reproduce the same structural weakness identified in Article 27 of the EU AI Act.

## LIST OF BIBLIOGRAPHY

**Books:**

1. Shevchenko, Anatolii I., ed. *Strategy for Artificial Intelligence Development in Ukraine: Monograph*. Kyiv: Institute of Artificial Intelligence Problems of NAS of Ukraine and MES of Ukraine, 2023.

https://doi.org/10.15407/development_strategy_2023

2. Siegmann, Charlotte, and Markus Anderljung. *The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market*. Oxford: Centre for the Governance of AI, 2022.

https://www.governance.ai/research-paper/brussels-effect-ai

3. Smuha, Nathalie A. *Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law*. Cambridge: Cambridge University Press, 2024.

https://doi.org/10.1017/9781009367783

**Chapters in edited volumes**

4. Bilokobylskyi, Oleksandr V. "To Section 3 'Aims and Objectives of the Strategy' and Section 6 'AI Governance System.'" In *Strategy for Artificial Intelligence Development in Ukraine: Monograph*, edited by Anatolii I. Shevchenko, 97-124. Kyiv: Institute of Artificial Intelligence Problems of the MES and NAS of Ukraine, 2023.

https://doi.org/10.15407/development_strategy_2023

5. Chebanov, Viktor B. "To Subsection 7.3 of Section 7 'Artificial Intelligence in Medicine.'" In *Strategy for Artificial Intelligence Development in Ukraine: Monograph*, edited by Anatolii I. Shevchenko, 239-242. Kyiv: Institute of Artificial Intelligence Problems of the MES and NAS of Ukraine, 2023.

https://doi.org/10.15407/development_strategy_2023

6. Kondratenko, Yuriy P., Oleksiy S. Striuk, Oleksii V. Kozlov, and Ievgen V. Sidenko. "To Section 1 'Paradigm.'" In *Strategy for Artificial Intelligence Development in Ukraine: Monograph*, edited by Anatolii I. Shevchenko, 126-148. Kyiv: Institute of Artificial Intelligence Problems of the MES and NAS of Ukraine, 2023.

https://doi.org/10.15407/development_strategy_2023

7. Götzmann, Nora. "Introduction to the *Handbook on Human Rights Impact Assessment*: Principles, Methods and Approaches." In *Handbook on Human Rights Impact Assessment*, edited by Nora Götzmann, 2-30. Cheltenham: Edward Elgar Publishing, 2019.

https://doi.org/10.4337/9781788970006

8. Ho-Dac, Marion. "Considering Fundamental Rights in the European Standardisation of Artificial Intelligence: Nonsense or Strategic Alliance?" In *Joint Proceedings EURAS & SIIT 2023: (Responsible) Standardisation for Smart Systems*, edited by Kai Jakobs, 131-150. Aachen: Mainz Verlag, 2023.

https://hal.science/hal-04411136/document

**Reports, working papers, and institutional studies**

9. Ajoodha, Thomas, and Jared Browne. *Fundamental Rights Impact Assessments: What Are They? How Do They Work?* CEDPO AI and Data Working Group Micro-Insights Series. Brussels: CEDPO, January 2025.

https://cedpo.eu/wp-content/uploads/CEDPO-micro-insight-paper-fundamental-rights-impact-assessments.pdf

10. Almada, Marco, and Nicolas Petit. *The EU AI Act: A Medley of Product Safety and Fundamental Rights?* EUI RSC Working Paper 2023/59. Florence: European University Institute, 2023.

https://doi.org/10.2870/342421

11. European Center for Not-for-Profit Law (ECNL) and SocietyInside. *Civil Society Guidance on Fundamental Rights Impact Assessments under the EU AI Act*. Brussels: ECNL, 2023.

https://ecnl.org/publications/guide-fundamental-rights-impact-assessments-fria

12. European Union Agency for Fundamental Rights. *Getting the Future Right - Artificial Intelligence and Fundamental Rights*. Luxembourg: Publications Office of the European Union, 2020.

https://doi.org/10.2811/774118

13. Gerards, Janneke, Mirko Tobias Schäfer, Iris Muis, and Arthur Vankan. *Fundamental Rights and Algorithms Impact Assessment (FRAIA)*. The Hague: Ministry of the Interior and Kingdom Relations, 2022.

https://www.government.nl/site/binaries/site-content/collections/documents/2021/07/31/impact-assessment-fundamental-rights-and-algorithms/fundamental-rights-and-algorithms-impact-assessment-fraia.pdf

14. Research Service of the Verkhovna Rada of Ukraine. *Analytical Note on Comparative Legislation Regarding the Legal Regulation of Artificial Intelligence Technologies in Ukraine, European States, and the USA*. Kyiv: Verkhovna Rada of Ukraine, 2025 [in Ukrainian].

https://research.rada.gov.ua/en/documents/page/documents/analyticRSmaterialsDocs_en/industry_policy_en/analytical_notes-indst_en/76671.html

**Periodicals**

*Includes journal articles, review articles, SSRN working papers and conference proceedings.*

15. Almada, Marco, and Anca Radu. "The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy." *German Law Journal* 25, 4 (2024): 646-663.

https://doi.org/10.1017/glj.2023.108

16. Augenstein, Daniel. "Engaging the Fundamentals: On the Autonomous Substance of EU Fundamental Rights Law." *German Law Journal* 14, 10 (2013): 1917-1944.

https://doi.org/10.1017/S2071832200002571

17. Binns, Reuben. "Data Protection Impact Assessments: A Meta-Regulatory Approach." *International Data Privacy Law* 7, 1 (2017): 22-35.

https://doi.org/10.1093/idpl/ipw027

18. Black, Julia, and Robert Baldwin. "Really Responsive Risk-Based Regulation." *Law & Policy* 32, 2 (2010): 181-213.

https://doi.org/10.1111/j.1467-9930.2010.00318.x

19. Bodnar, Kateryna. "Regulatory Adaptation of Personal Data Protection Standards to Hybrid Threats in the EU and Ukraine." *Pressing Problems of Public Administration* 2, 67 (2025): 419-436 [in Ukrainian].

https://doi.org/10.26565/1684-8489-2025-2-21

20. Bowie, Norman E. Review of *Taking Rights Seriously*, by Ronald Dworkin. *Catholic University Law Review* 26, 4 (1977): 908-923.

21. Bradford, Anu. "The Brussels Effect." *Northwestern University Law Review* 107, 1 (2012): 1-68.

https://scholarship.law.columbia.edu/faculty_scholarship/271/

22. De Cooman, Jérôme. "Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act." *Market and Competition Law Review* 6, 1 (2022): 49-90.

https://doi.org/10.34632/mclawreview.2022.11304

23. de Vries, Sybe, Olia Kanevskaia, and Rik de Jager. "Internal Market 3.0: The Old 'New Approach' for Harmonising AI Regulation." *European Papers* 8, 2 (2023): 583-610.

https://doi.org/10.15166/2499-8249/651

24. Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act." *European Journal of Risk Regulation* 16, 2 (2025): 684-703.

https://doi.org/10.1017/err.2024.78

25. Gatt, Lucilla, Ilaria Amelia Caggiano, Maria Cristina Gaeta, Emiliano Troisi, Roberta Savella, Francesca Pratesi, and Roberto Trasarti. "FRIA Implementation Model According to the AI Act." *European Journal of Privacy Law & Technologies* 2 (2024): 192-204.

https://doi.org/10.57230/EJPLT.24.2.LGIACMCGETRSRTFP

26. Gellert, Raphaël. "The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?" *Journal of Ethics and Legal Technologies* 3, 2 (2021): 15-33.

https://jelt.padovauniversitypress.it/2021/2/2

27. Gill-Pedro, Eduardo. "Fundamental Rights Impact Assessments in the EU's AI Act: A Teleological and Contextual Analysis of the Obligations of Deployers." *European Journal of Law and Technology* 16, 3 (2025): 1-24.

https://ejlt.org/index.php/ejlt/article/view/1065

28. Götzmann, Nora. "Human Rights Impact Assessment of Business Activities: Key Criteria for Establishing a Meaningful Practice." *Business and Human Rights Journal* 2, 1 (2017): 87-108.

https://doi.org/10.1017/bhj.2016.17

29. Gstrein, Oskar J. "European AI Regulation: Brussels Effect versus Human Dignity?" *Zeitschrift für Europarechtliche Studien* 25, 4 (2022): 755-772.

https://www.inlibra.com/de/document/view/pdf/uuid/e8084104-c581-38db-906f-b1a12c6f56f5

30. Hura, Maksym. "Adaptation of Ukrainian Legislation to the Norms of the EU Artificial Intelligence Act: Challenges and Prospects." *The Journal of V. N. Karazin Kharkiv National University, Series "Law"* 40 (2025): 119-128 [in Ukrainian].

https://periodicals.karazin.ua/law/article/view/27640

31. Janssen, Heleen, Michelle Seng Ah Lee, and Jatinder Singh. "Practical Fundamental Rights Impact Assessments." *International Journal of Law and Information Technology* 30, 2 (2022): 200-232.

https://academic.oup.com/ijlit/article/30/2/200/6835507

32. Justo-Hanani, Ronit. "Risk-Based Approach to EU AI Act: Benefits and Challenges of Co-Regulation." *Policy Design and Practice* 9, 2 (2026): 1-10.

https://doi.org/10.1080/25741292.2025.2610869

33. Kaminski, Margot E. "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability." *Southern California Law Review* 92 (2019): 1529-1616.

https://scholar.law.colorado.edu/faculty-articles/1265/

34. Kaminski, Margot E. "Regulating the Risks of AI." *Boston University Law Review* 103 (2023): 1347-1411.

https://www.bu.edu/bulawreview/files/2023/11/KAMINSKI.pdf

35. Karathanasis, Theodoros. *The FRIA in EU AI Act: Governance, Rights, and Global Jurisdiction*. SSRN Working Paper, July 5, 2025: 1-19.

https://doi.org/10.2139/ssrn.5340079

36. Komarova, Tetyana, and Adam Łazowski. "Switching Gear: Law Approximation in Ukraine after the Application for EU Membership." *Croatian Yearbook of European Law and Policy* 19 (2023): 105-132.

https://doi.org/10.3935/cyelp.19.2023.532

37. Lasek-Markey, Marta, and Linda Hogan. "Delivering on the Promise of the Fundamental Rights Impact Assessments in the EU AI Act: Intersectionality and Vulnerability." *European Journal of Law and Technology* 16, 2 (2025): 1-23.

https://ejlt.org/index.php/ejlt/article/view/1124

38. Lenaerts, Koen. "Exploring the Limits of the EU Charter of Fundamental Rights." *European Constitutional Law Review* 8, 3 (2012): 375-403.

https://doi.org/10.1017/S1574019612000260

39. Malgieri, Gianclaudio, and Frank Pasquale. *From Transparency to Justification: Toward Ex Ante Accountability for AI*. SSRN Working Paper, 2022: 1-27.

https://doi.org/10.2139/ssrn.4099657

40. Mantelero, Alessandro. "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment." *Computer Law & Security Review* 34, 4 (2018): 754-772.

https://doi.org/10.1016/j.clsr.2018.05.017

41. Mantelero, Alessandro. "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template." *Computer Law & Security Review* 54 (2024): 1-18.

https://doi.org/10.1016/j.clsr.2024.106020

42. Mantelero, Alessandro, and Maria Samantha Esposito. "An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems." *Computer Law & Security Review* 41 (July 2021): 1-35.

https://doi.org/10.1016/j.clsr.2021.105561

43. McGregor, Lorna, Daragh Murray, and Vivian Ng. "International Human Rights Law as a Framework for Algorithmic Accountability." *International and Comparative Law Quarterly* 68, 2 (2019): 309-343.

https://doi.org/10.1017/S0020589319000046

44. Mökander, Jakob, Jonas Schuett, Hannah Rose Kirk, and Luciano Floridi. "Auditing Large Language Models: A Three-Layered Approach." *AI and Ethics* 4, 4 (2024): 1085-1115.

https://doi.org/10.1007/s43681-023-00289-2

45. Muir, Elise. "Fundamental Rights: An Unsettling EU Competence." *Human Rights Review* 15, 1 (2014): 25-37.

https://doi.org/10.1007/s12142-013-0295-x

46. Novelli, Claudio, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo, and Luciano Floridi. "AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act." *Digital Society* 3, 1 (2024): 1-29.

https://doi.org/10.1007/s44206-024-00097-x

47. Parkhomenko, Nataliia, Svitlana Podorozhna, Tetiana Tarakhonych, Stanislav Husarev, and Diana Biloskurska. "Implementation of the Association Agreement with the EU by Adapting Ukrainian Legislation to EU Law." *Social & Legal Studios* 7, 1 (2024): 184-193 [in Ukrainian].

https://doi.org/10.26693/jls2024.01.184

48. Perederii, Oleksandr. "Legal Principles of the Use of Artificial Intelligence in Ukraine in the Context of the Europeanization of the National Legal System." *The Journal of V. N. Karazin Kharkiv National University, Series "Law"* 40 (2025): 55-61 [in Ukrainian].

https://doi.org/10.26565/2075-1834-2025-40-05

49. Petrov, Roman. "Approximation of Laws in the EU-Ukraine Association Agreement." *Naukovi Zapysky NaUKMA: Juridical Sciences* 155 (2014): 24-26.

https://ekmair.ukma.edu.ua/server/api/core/bitstreams/f2853e61-d2db-4acf-a282-21883a8c3d3e/content

50. Schuett, Jonas. "Risk Management in the Artificial Intelligence Act." *European Journal of Risk Regulation* 15, 2 (2024): 367-385.

https://doi.org/10.1017/err.2023.1

51. Spaventa, Eleanor. "The Interpretation of Article 51 of the EU Charter of Fundamental Rights: The Dilemma of Stricter or Broader Application of the Charter to National Measures." Study PE 556.930. *Brussels: European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs*, 2016: 1-38.

https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2016)556930

52. Stahl, Bernd Carsten, Josephina Antoniou, Nitika Bhalla, Laurence Brooks, Philip Jansen, Blerta Lindqvist, Alexey Kirichenko, Samuel Marchal, Rowena Rodrigues, Nicole Santiago,

Zuzanna Warso, and David Wright. "A Systematic Review of Artificial Intelligence Impact Assessments." *Artificial Intelligence Review* 56, 11 (2023): 12799-12831.

https://doi.org/10.1007/s10462-023-10420-8

53. Toner, Helen. "Impact Assessments and Fundamental Rights Protection in EU Law." *European Law Review* 31, 3 (2006): 316-341.

https://scispace.com/pdf/impact-assessments-and-fundamental-rights-protection-in-eu-ftif66qm7j.pdf

54. Wachter, Sandra. "Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond." *Yale Journal of Law & Technology* 26, 3 (2024): 671-718.

https://yjolt.org/limitations-and-loopholes-eu-ai-act-and-ai-liability-directives-what-means-european-union-united

55. Wernick, Alina. "Impact Assessment as a Legal Design Pattern - A 'Timeless Way' of Managing Future Risks?" *Digital Society* 3, 2 (2024): 1-36.

https://doi.org/10.1007/s44206-024-00111-4

56. Yeung, Karen, and Lee A. Bygrave. "Demystifying the Modernised European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship." *Law, Innovation and Technology* 14 (2022): 137-230.

https://doi.org/10.1080/17579961.2022.2113671

57. Yukhymenko, Stanislav. *Analytical Note: AI Regulation - EU Experience and Future Regulation in Ukraine*. Kyiv: Institute for Economic Research and Policy Consulting, 2025: 1-18 [in Ukrainian].

http://www.ier.com.ua/files/Projects/2025/UA_EU/Регулювання_штучного_інтелекту.pdf

**Legal Acts**

*Includes EU regulations, directives, treaties, the Charter, institutional proposals and staff working documents; Ukrainian laws, constitutional texts, draft laws, concept papers and strategy documents; Council of Europe conventions, recommendations, and guidance instruments.*

58. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679." Article 29 Data Protection Working Party, WP 248 rev.01. October 4, 2017.

https://ec.europa.eu/newsroom/article29/items/611236

59. "Association Agreement between the European Union and the European Atomic Energy Community and Their Member States, of the One Part, and Ukraine, of the Other Part." *Official Journal of the European Union* L 161, May 29, 2014.

https://www.kmu.gov.ua/en/yevropejska-integraciya/ugoda-pro-asociacyu

60. "Charter of Fundamental Rights of the European Union." *Official Journal of the European Union* C 326, October 26, 2012: 391-407.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

61. "Commission Staff Working Document: Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." European Commission, SWD(2021) 84 final. Brussels, April 21, 2021.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0084

62. "Constitution of Ukraine." Verkhovna Rada of Ukraine, adopted June 28, 1996, as amended [in Ukrainian].

https://zakon.rada.gov.ua/laws/show/254к/96-вр

63. "Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (Oviedo Convention)." Council of Europe, European Treaty Series No. 164. April 4, 1997.

https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=164

64. "Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law." Council of Europe Treaty Series No. 225. Vilnius, September 5, 2024.

https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225

65. "Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859." *Official Journal of the European Union* L, July 5, 2024: 1-58.

https://eur-lex.europa.eu/eli/dir/2024/1760/oj

66. "Directive on Automated Decision-Making." Treasury Board of Canada Secretariat. Ottawa, 2019, amended 2025.

https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

67. "Draft Law of Ukraine on Personal Data Protection." Verkhovna Rada of Ukraine, Bill No. 8153. October 25, 2022 [in Ukrainian].

https://itd.rada.gov.ua/billInfo/Bills/Card/40707

68. "EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." European Data Protection Board and European Data Protection Supervisor. Brussels, June 18, 2021.

https://www.edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

69. "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework." United Nations, HR/PUB/11/04. New York and Geneva, 2011.

https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

70. OECD. *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Paris: OECD, 2019, updated 2024.

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

71. "On Approval of the Concept for the Development of Artificial Intelligence in Ukraine." Cabinet of Ministers of Ukraine, Resolution No. 1556-r of December 2, 2020, as amended by Resolution No. 1787-r of December 29, 2021 [in Ukrainian].

https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text

72. "Opinion 44/2023 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act)." European Data Protection Supervisor. Brussels, 2023.

https://www.edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinion_en.pdf

73. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." European Commission, COM(2021) 206 final. Brussels, April 21, 2021.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

74. "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, and Repealing Directive 95/46/EC (General Data Protection Regulation)." *Official Journal of the European Union* L 119, May 4, 2016: 1-88.

https://eur-lex.europa.eu/eli/reg/2016/679/oj

75. "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." *Official Journal of the European Union* L, 2024/1689, July 12, 2024.

https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

76. "Treaty on European Union (Consolidated Version)." *Official Journal of the European Union* C 326, October 26, 2012: 13-45.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT

77. "Treaty on the Functioning of the European Union (Consolidated Version)." *Official Journal of the European Union* C 326, October 26, 2012: 47-390.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT

78. "White Paper on Artificial Intelligence - A European Approach to Excellence and Trust." European Commission, COM(2020) 65 final. Brussels, February 19, 2020.

https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

79. "White Paper on Artificial Intelligence Regulation in Ukraine." Ministry of Digital Transformation of Ukraine. Kyiv, 2024.

https://storage.thedigital.gov.ua/files/c/fc/36c4cae89deedfbf3781ec6bceddffcc.pdf

**Case-law**

80. "Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González." Court of Justice of the European Union, ECLI:EU:C:2014:317. Judgment of May 13, 2014.

https://curia.europa.eu/juris/liste.jsf?num=C-131/12

81. "Case C-176/12, Association de médiation sociale v. Union locale des syndicats CGT and Others." Court of Justice of the European Union, ECLI:EU:C:2014:2. Judgment of January 15, 2014.

https://curia.europa.eu/juris/liste.jsf?num=C-176/12

82. "Case C-414/16, Vera Egenberger v. Evangelisches Werk für Diakonie und Entwicklung e.V." Court of Justice of the European Union, ECLI:EU:C:2018:257. Judgment of April 17, 2018.

https://curia.europa.eu/juris/liste.jsf?num=C-414/16

83. "Joined Cases C-267/91 and C-268/91, Criminal Proceedings against Bernard Keck and Daniel Mithouard." Court of Justice of the European Union, ECLI:EU:C:1993:905. Judgment of November 24, 1993.

https://curia.europa.eu/juris/liste.jsf?num=C-267/91

**Websites**

84. "How Ukraine Will Develop AI Strategy till 2030 - the Draft Was Presented." Ministry of Digital Transformation of Ukraine, thedigital.gov.ua. Accessed April 2026 [in Ukrainian].

https://thedigital.gov.ua/news/technologies/iak-ukrayina-rozvyvatyme-shi-do-2030-roku-prezentuvaly-proyekt-stratehiyi

## ABSTRACT

This thesis asks whether the Fundamental Rights Impact Assessment (FRIA) under Article 27 of Regulation (EU) 2024/1689 actually protects fundamental rights before high-risk AI is deployed, or whether it ends up as a paper exercise - and what design lessons follow for Ukraine. The study sets out the constitutional foundation of the AI Act under Article 114 TFEU and the New Legislative Framework, traces the relationship between high-risk AI deployment and the Charter of Fundamental Rights, and draws normative criteria from the Data Protection Impact Assessment under Article 35 GDPR and from the Human Rights Impact Assessment tradition. It then analyses Article 27 doctrinally and compares it against the HRIA and DPIA, the Dutch FRAIA, the Canadian Directive on Automated Decision-Making, and the Corporate Sustainability Due Diligence Directive. The central finding is that Article 27 is built in a way that pushes deployers toward box-ticking: it satisfies none of the four HRIA process criteria as binding legal requirements and only partly meets the content criteria. The thesis turns that diagnosis into a connected set of seven design choices for Ukraine, grounded in Articles 3 and 22 of the Constitution and tailored to Draft Law No. 8153, the National AI Concept, and wartime institutional capacity. It shows that approximation under Article 474 of the EU-Ukraine Association Agreement requires Ukraine to reach the same protective result as EU law, which permits (and in fact calls for) a Ukrainian FRIA stronger than its EU model.



**Keywords**: Fundamental Rights Impact Assessment; EU AI Act; Ukraine; high-risk AI; legal approximation.

## SUMMARY

**Title of the thesis**: Fundamental Rights Impact Assessment as Human Rights Protection Tool under EU AI Act.

The thesis addresses the following research problem: does the Fundamental Rights Impact Assessment under Article 27 of Regulation (EU) 2024/1689 actually protect fundamental rights before high-risk AI is deployed, or is it built in a way that pushes deployers toward formal compliance, and what design lessons follow for Ukraine as it adapts its legal framework to the EU acquis under the Association Agreement. The aim of the research is to determine how protective Article 27 really is and, on that basis, to develop a coherent and constitutionally grounded design template for a Ukrainian FRIA. The thesis pursues three objectives: (1) to set out the criteria against which Article 27 must be measured by reconstructing the constitutional basis of the AI Act, the rights at stake under the Charter, and the methodological standards developed in the impact assessment tradition; (2) to identify the structural weaknesses of Article 27 through doctrinal analysis and systematic comparison with the HRIA and the DPIA; and (3) to propose, on the basis of that analysis and a comparison with the Dutch FRAIA, the Canadian Directive on Automated Decision-Making, and the CSDDD, a set of legislative design choices for a FRIA-type obligation suited to Ukraine's constitutional framework, Draft Law No. 8153, and current institutional capacity.

The structure follows this logic. Chapter I builds the conceptual and normative framework: how the AI Act and Article 27 came about; the relationship between high-risk AI systems and the Charter; the Brussels Effect compared with Ukraine's binding approximation duty; and the development of impact assessment from environmental and data-protection origins through to the HRIA. Chapter II is the doctrinal core: it analyses the legal nature, scope, methodology, supervision, and enforcement of Article 27; runs a process-and-content comparison against the HRIA criteria of Götzmann and of Lasek-Markey and Hogan and against the DPIA under Article 35 GDPR; and brings together the structural critiques in the scholarship into a single diagnostic framework that bridges into Chapter III. Chapter III develops the proposal for Ukraine: it maps the legislative baseline, sets out seven connected design choices each tied to one of the seven diagnosed weaknesses, and proposes a hybrid supervisory architecture with a staged, wartime-calibrated implementation plan. Conclusions and Recommendations turn the analysis into proposals addressed to the Ukrainian legislator and to the supervisory authorities responsible for AI governance.

The principal results of the research are six. First, the function of the FRIA is shaped not by Article 27 alone but by three factors working together - the broad and context-dependent nature of the Charter rights engaged by high-risk AI deployment; the New Legislative Framework product-safety architecture, built on Article 114 TFEU, which places rights protection below market integration not because the legal basis demands it but because of the regulatory model chosen on that basis; and the different character of Ukraine's approximation obligation under the Association Agreement, which works by legal duty rather than by market incentive. Second, the criteria for evaluating Article 27 do not come from the AI Act itself but from the impact-assessment tradition - in particular Article 35 GDPR, the UN Guiding Principles on Business and Human Rights, and the methodological work of Mantelero and Götzmann; an adequate impact assessment must be human-rights informed, participatory, intersectional, transparent, and iterative. Third, Article 27 has seven structural weaknesses that reinforce each other (product-safety mismatch, narrow personal scope, methodological vacuum, institutional misfit, enforcement deficit, assessment fragmentation, and participatory deficit) and these are not separate drafting errors but joint consequences of inserting a rights-protection function into an internal-market instrument. Fourth, comparing Article 27 criterion by criterion with the HRIA and the DPIA shows that the FRIA satisfies none of the process criteria of participation, non-discrimination, empowerment, and accountability as binding legal requirements, and only partly the content criteria; the box-ticking risk is therefore built into the design, not just a question of how the rule is applied. Fifth, Ukraine's approximation duty under Article 474 of the Association Agreement requires reaching the same protective result as EU law, which permits (and in fact calls for) a Ukrainian FRIA that fixes the seven weaknesses rather than copying them; a constitutionally anchored, methodologically prescribed, participatory and enforceable Ukrainian FRIA would be more in line with the rights-protective aim of Article 1 of the AI Act than a verbatim transposition. Sixth, the seven design choices developed for Ukraine form a connected system (constitutional anchoring enables universal scope, universal scope requires a prescribed methodology, methodology requires rights-competent supervision, supervision requires binding enforcement, and an integrated architecture prevents assessment fragmentation). Implementing only part of the package undermines the rest.

Taken together, these findings confirm the thesis defense statements. The FRIA in its current form cannot deliver the rights protection that the AI Act assigns to it, because the structural choices made under Article 114 TFEU and the New Legislative Framework leave rights as a secondary constraint on market integration. For Ukraine, the legislative window

opened by the parallel preparation of Draft Law No. 8153 and the developing AI legislation makes it possible to design a constitutionally enriched FRIA that learns from and corrects the structural weaknesses of the EU model before enactment, rather than carrying them across into Ukrainian law