

T

Marta Fasan

The Fundamental Rights Impact Assessment: Lights and Shadows in Protecting Fundamental Rights in the Field of Artificial Intelligence*

1. *Untying the knot. New regulatory approaches in the definition of artificial intelligence legal framework*

The complex relationship between the legal domain and the scientific-technological sphere lies at the heart of contemporary debates in public law scholarship, both at the national level and, increasingly, within supranational and international contexts¹.

It has long been evident that the outcomes of scientific and technological innovation have a significant influence on the social and relational structures that shape society as a whole. These transformations constitute one of the main challenges facing modern legal systems, which are required to respond through their own traditional tools, categories, and methods². Yet, this task is far from straightforward, given the fundamental differences

* This paper constitutes an update of the subject matter previously delineated in M. Fasan, *I meccanismi di valutazione d'impatto nel prisma della tutela dei diritti fondamentali. Un'analisi in prospettiva comparata in materia di intelligenza artificiale*, in «BioLaw Journal - Rivista di BioDiritto», 2 (2025), pp. 183-198.

¹ R. Brownsword, H. Somsen, *Law, innovation and technology: fast forward to 2021*, in «Law, Innovation and Technology», 1 (2021), pp. 1-28; L. Bennet Moses, *How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target*, in «Law, Innovation and Technology», 1 (2013), pp. 1-20. Among Italian legal scholars cfr. E. D'Orlando, *Decisore politico e scienza: l'emergenza sanitaria come catalizzatore dell'affermazione di un paradigma normativo evidence-based*, in «DPCE online», 1 (2023), pp. 511-535; S. Penasa, *Alla ricerca di un lessico comune: inte(g)razioni tra diritto e scienze della vita in prospettiva comparata*, in «DPCE online» 3 (2020), p. 3312.

² L. Bennet Moses, *Why Have a Theory of Law and Technological Change?*, in «Minnesota Journal of Law, Science & Technology», 2 (2007), pp. 589-606; S. Rodotà, *Tecnologie e diritti*, il Mulino, Bologna 2021, p. 146 ff.

that distinguish the legal sphere from the technological-scientific one.

Law, in order to fulfil its constitutional function of “measuring” and constraining power for the protection of fundamental rights³, must ensure a sufficient degree of predictability and stability in the production of norms aimed at governing social behaviours, as well as a broad level of consensus regarding their content⁴. Conversely, the characteristics that define the scientific-technological phenomenon as an object of regulation differ remarkably. On the one hand, the products of scientific and technological innovation are technically complex, both in their terminology and in their operational mechanisms, thereby limiting accessibility and full comprehension for non-experts in the field⁵. On the other hand, scientific and technological phenomena evolve at a significant pace, continuously transforming the functionalities and solutions offered by technological products and processes⁶.

These elements, which permeate the relationship between law and technology, become even more evident when examining the role that law can play in regulating artificial intelligence (AI).

AI technologies are demonstrating their ability to pervasively reshape society and its inner structures, to the extent that they can mould a new model of “algorithmic society” which is «(...) organized around social and economic decision-making, who do not only make the decisions but also, in some cases, carry them out»⁷. This phenomenon gives rise to new legal issues, determined by both the technological features of AI and its social impact, and new protection requirements that the law need to address through

³ A. Simoncini, *Sovranità e potere nell'era digitale*, in T.E. Frosini et al. (eds), *Diritti e libertà in internet*, Mondadori Education, Firenze 2019, p. 20 ff.; C. Casonato, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in «Diritto Pubblico Comparato ed Europeo», Special issue (2019), pp. 101-130; R. Toniatti, *Common Law Constitutionalism*, in «Costituzionalismo britannico e irlandese», 2 (2024), p. 6 ff.

⁴ L. Reins, *Regulating New Technologies in Uncertain Times - Challenges and Opportunities*, in L. Reins (ed.), *Regulating New Technologies in Uncertain Times*, Springer, The Hague 2019, p. 20.

⁵ C. Casonato, *The Essential Features of 21st Century Biolaw*, in E. Valdés, J.A. Lecaros (eds), *Biolaw and Policy in the Twenty-First Century. Building Answers for New Questions*, Springer, Cham 2019, p. 77 ff.

⁶ R. Brownsword, *Rights, Regulation, and the Technological Revolution*, Oxford University Press, Oxford 2008, pp. 162-165. Among Italian legal scholars see also A. Iannuzzi, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, Napoli 2018, pp. 3-4; S. Penasa, *La legge della scienza: nuovi paradigmi dell'attività medico-scientifica. Uno studio comparato in materia di procreazione medicalmente assistita*, Editoriale Scientifica, Napoli 2015, p. 29 ff.

⁷ J.M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in «Ohio State Law Journal», 5 (2017), p. 1219.

the definition of principles, rules and obligations to regulate the development and use of AI⁸.

Nevertheless, the definition of legal frameworks for AI regulation continues to represent a remarkably challenge.

The inherent complexity of AI systems, the rapidity of scientific progress in this domain, and the AI de-spatialized nature, which raise substantial challenges concerning the territorial scope of applicable regulations⁹, have, in recent years, revealed the potential inadequacies of traditional legal categories and instruments in effectively governing AI. These limitations emerge both in the need to provide adequate support for innovation and in the imperative to safeguard the rights of individuals who interact with AI systems¹⁰.

This awareness has prompted legislative bodies to complement traditional regulatory frameworks with novel approaches and tools. These new strategies increasingly rely on the participation of technological actors and the private sector, recognizing the potential of these agents to contribute to responsive and adaptive regulatory practices. From this perspective, it is unsurprising that recent regulatory acts on AI provide forms of delegated regulation, through by-design solutions and self-regulatory measures, within broader political and legislative frameworks. Such developments give rise to hybrid forms of co-regulation, which employ specific mechanisms and procedures to ensure both the promotion and protection of the diverse interests related to the development and deployment of AI systems¹¹.

⁸ G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge 2022; O. Pollicino, G. De Gregorio, *Constitutional Law in the Algorithmic Society*, in H.-W. Micklitz et al. (eds), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge 2022, p. 5 ff.

⁹ A. Garapon, *La despatializzazione della giustizia*, Mimesis, Milano-Udine 2021.

¹⁰ O. Pollicino, *The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism*, in «European Law Journal», 14 August 2023, pp. 1-21.

¹¹ L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York 1999; R. Brownsword, *Law 3.0*, Routledge, Abingdon-New York 2020, p. 28; K. Yeung, *Towards an Understanding of Regulation by Design*, in R. Brownsword, K. Yeung (eds), *Regulating Technologies. Legal Features, Regulatory Frames and Technological Fixes*, Oxford University Press, Oxford-Portland 2008, p. 81 ff.; N. Gunningham, J. Rees, *Industry Self-Regulation: An Institutional Perspective*, in «Law & Policy», 4 (1997), p. 364 ff. Among Italian legal scholars cfr. A. Iannuzzi, *Paradigmi normativi per la disciplina della tecnologia: auto-regolazione, co-regolazione ed etero-regolazione*, in «Bilancio, Comunità, Persona», 2 (2023), p. 91 ff.; A. Simoncini, *La co-regolazione delle piattaforme digitali*, in «Rivista trimestrale di diritto pubblico», 4 (2022), p. 1031 ff.; G. Mobilio, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in «Bio-Law Journal - Rivista di BioDiritto», 2 (2020), pp. 415-418.

2. *Impact assessment as a “new” tool for the protection of fundamental rights in the field of artificial intelligence*

The adoption of co-regulatory approaches in the governance of artificial intelligence, aimed at fostering synergy between public-institutional and private regulatory dimensions, is most clearly expressed by impact assessment tools. This specific type of legal mechanism is proving to be quite successful in the legislative frameworks designed to regulate the development and use of AI, due to the distinctive features that characterise its operation and implementation.

In regulatory terms, impact assessment is a tool that facilitates the interaction between public authorities and private actors in evaluating the potential effects that a specific activity, process, or technological product may have on a defined set of protected interests and values. This mechanism can be situated within the broader category of Technology Assessment, a concept first developed in the United States during the latter half of the twentieth century to describe the assessment practices carried out by policymakers on the societal impacts of emerging technologies¹². Although originally conceived as a self-regulation tool related to environmental protection¹³, impact assessment has progressively evolved into an adaptable tool, that may be applied to different domains, including the safeguard of people’s rights. Over time, it has come to play a pivotal role not only in safeguarding general human rights¹⁴ but also in addressing specific legal interests, such as the right to health¹⁵, the right to data protection¹⁶,

¹² Cfr. D. Banta, *What is Technology Assessment*, in «International Journal of Technology Assessment in Health Care», 1 (2009), pp. 7-9.

¹³ J. Glasson, R. Therivel, *Introduction to Environmental Impact Assessment*, Taylor & Francis, London 2013.

¹⁴ R. Boele, C. Crispin, *What direction for human rights impact assessments?*, in «Impact Assessment and Project Appraisal», 2 (2013), pp. 128-134; G. De Beco, *Human Rights Impact Assessments*, in «Netherlands Quarterly of Human Rights», 27 (2009), p. 139 ff.; D. Kemp, F. Vanclay, *Human rights and impact assessment: clarifying the connections in practice*, in «Impact Assessment and Project Appraisal», 2 (2013), pp. 86-96; A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Springer, The Hague 2022, p. 15 ff.

¹⁵ B. Harris-Roxas *et al.*, *Health Impact Assessment: The State of the Art*, in «Impact assessment and project appraisal», 12 (2009), p. 43 ff.

¹⁶ D. Wright, *The State of the Art in Privacy Impact Assessment*, in «Computer Law & Security Review», 28 (2012), p. 54 ff.; G. Georgiadis, G. Poels, *Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: a systematic literature review*, in «Computer Law & Security Review», 44 (2022), pp. 1-21.

sustainability rights¹⁷ and the right to intergenerational equality¹⁸.

In the European Union context, impact assessment has undergone a process of full institutionalisation and recognition as a tool for safeguarding interests within EU legislation. First introduced by directives mandating environmental impact evaluations for public and private projects that could affect constitutionally protected environmental values¹⁹, impact assessment has then been embedded into other regulatory acts, such as data protection regulation²⁰, health technology assessment one²¹, and corporate due diligence regulation²². This evolution transformed impact assessment from a mechanism of private self-regulation into a cornerstone of co-regulation, whereby legislative authorities define the objectives and parameters of assessment, and regulated entities are responsible for analysing and managing the impacts of their activities, economic, technological, or otherwise, within that established framework²³.

As a result, impact assessment has become an essential component of regulatory interventions in technologically complex and rapidly evolving fields, such as digital innovation and AI. In these areas, the active involvement of regulated entities is essential to identifying legally sound solutions that ac-

¹⁷ H.-J. De Kluiver, *Towards a framework for effective regulatory supervision of sustainability governance in accordance with the EU CSDD Directive. A comparative study*, in «European Company and Financial Law Review», 1 (2023), pp. 203-239; F. Rohde *et al.*, *Broadening the perspective for sustainable artificial intelligence: sustainability criteria and indicators for Artificial Intelligence systems*, in «Current Opinion in Environmental Sustainability», 66 (2024), pp. 1-12.

¹⁸ R.E. Parsons, L.K. Mottee, *Exploring equity in social impact assessment*, in «Current Sociology», 4 (2024), pp. 732-752. Among Italian legal scholars cfr. L. Bartolucci, *La valutazione di impatto generazionale delle leggi come forma di attuazione degli artt. 9 e 97 Cost.*, in «Federalismi.it», 4 (2024), pp. 39-49.

¹⁹ Directive 85/337/EEC (subsequently amended by Directive 97/11/EC, Directive 2003/35/EC and Directive 2009/31/EC) and Directive 2011/92/EU, which was also amended in 2014 by Directive 2014/52/EU.

²⁰ 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).

²¹ Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU.

²² 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.

²³ A.M. Esteves, D. Franks, F. Vanclay, *Social impact assessment: the state of the art*, in «Impact Assessment and Project Appraisal», 1 (2012), pp. 34-42; A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, cit., p. 15 ff.; P.G. Chiara, F. Galli, *Normative Considerations on Impact Assessments in EU Digital Policy*, in «MediaLaws - Rivista di Diritto dei Media», 1 (2024), p. 86 ff.

count for the technical and operational complexity of these technologies²⁴.

Moreover, the growing significance of impact assessment with respect to AI regulation can be explained by two additional considerations.

First, impact assessment is inherently aligned with the risk-based regulatory approach, which has become the dominant paradigm in both digital governance and AI regulation²⁵. This approach seeks to avoid excessive and overburdening regulation by tailoring legal obligations according to the level of risk a given activity poses to protected societal interests and values²⁶. In this framework, the intensity of regulation, ranging from the lack of rules to outright prohibitions, increases proportionally to the level of foreseeable risk and its potential effects²⁷. Consequently, impact assessment becomes a crucial mechanism for operationalizing this approach: by identifying and evaluating the impacts of AI technologies, it enables a more specific determination of risk levels and their implications for legally protected interests²⁸.

Second, impact assessment provides a concrete analytical framework for examining the real-world consequences of AI applications. Because it is typically conducted by those directly involved in the development or deployment of AI, namely, the deployers themselves, the assessment reflects the specific operational context and tangible outcomes of AI technologies. This contextualized analysis complements the general and abstract nature of legislative intervention, thereby reducing the risk of overregulation and ensuring that restrictive measures are applied only where and when needed²⁹.

²⁴ S. Penasa, *Diritto e tecnologia nella recente riflessione giuridica comparata: "etichette" concettuali, sistemi di produzione normativa e metodi della comparazione*, in «Diritto pubblico comparato ed europeo», Special Issue (2024), p. 959 ff.

²⁵ J. Black, R. Baldwin, *When risk-based regulation aims low: approaches and challenges*, in «Regulation & Governance», 1 (2012), pp. 2-22; A. Alemanno, *Regulating the European Risk Society*, in A. Alemanno et al. (eds), *Better Business Regulation in a Risk Society*, Springer, New York 2012, p. 37 ff.

²⁶ M. Macenaite, *The "Riskification" of European Data Protection Law through a two-fold Shift*, in «European Journal of Risk Regulation», 8 (2017), pp. 506-540.

²⁷ C. Quelle, *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach*, in «European Journal of Risk Regulation», 9 (2018), pp. 502-526.

²⁸ P. Dunn, G. De Gregorio, *The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies*, in D. Dushi et al. (eds), *Proceedings of the Workshop on Imaging the AI Landscape after the AI Act (IAIL 2022)*, CEUR Workshop Proceedings, Amsterdam 2022, pp. 1-9; M. Ebers, *Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU's AI Act*, in «European Journal of Risk Regulation», 6 November 2024, pp. 1-20.

²⁹ C. Casonato, *A Brief Introduction*, in L. Antonioli, F. Cortese, E. Ioriatti, B. Marchetti (eds), *Trento e la comparazione giuridica: voci, esperienze, riflessioni. Dalla testimonianza di Ro-*

Considering these features, the inclusion of impact assessment within AI regulatory frameworks arises as a rational and effective means of protecting fundamental rights. The mechanism facilitates the balance, both abstract and concrete, between competing interests due to the pervasive use of AI systems. It allows policymakers and deployers to account for the specificities of each use case, ensuring that protective measures are tailored to the actual risks involved rather than imposed indiscriminately. In doing so, impact assessment enables the legal system to mitigate negative consequences without unduly hindering technological innovation³⁰.

However, the ability of impact assessment to guarantee the protection of fundamental rights is not an inherent or automatic quality of the mechanism itself. Its effectiveness depends on the precision with which legislation defines its scope, parameters, and implementation procedures. Without such clarity, the mechanism risks losing its normative and protective function, becoming an empty formal requirement unable of achieving the co-regulatory goals that justify its adoption.

3. *Impact assessment mechanisms in the regulation of artificial intelligence. Potential insights from a comparative law perspective*

The importance of embedding impact assessment within a clearly defined regulatory framework, one that specifies how private entities are to conduct such assessments to make them effective tools for the protection of fundamental rights, becomes more evident when examining the legislation that governs the use of artificial intelligence and mandates its implementation. From this standpoint, a comparative legal analysis proves to be the most effective method for identifying both the strengths and the shortcomings that characterize the legal and constitutional design of impact assessment as a tool for regulating AI systems and ensuring the protection of fundamental rights³¹.

dolfo Sacco e Mauro Cappelletti, Editorial Scientifica, Trento 2024, p. 227 ff.; A. Mantelero, *AI and Big Data: a blueprint for a human rights, social and ethical impact assessment*, in «Computer Law & Security Review», 4 (2018), pp. 754-772.

³⁰ A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template*, in «Computer Law & Security Review», 54 (2024), p. 1 ff.

³¹ G. Guerra, *An Interdisciplinary Approach for Comparative Lawyers: Insights from the Fast-Moving Field of Law and Technology*, in «German Law Journal», 3 (2018), pp. 579-612. Among Italian legal scholars cfr. A. Vendaschi, *Tecnologia, counter-terrorism e diritti*, in «Diritto pub-

In this regard, three legal systems serve as paradigmatic cases for analysis: Canada, the United States, and the European Union. Each legal system has developed regulatory tools which, though varying in scope and regulatory depth, share the common feature of recognising impact assessment as a central mechanism for protecting both legal interests and fundamental rights potentially affected by AI. At the same time, significant divergences among these systems reveal distinctive regulatory trends and differing conceptions of the function ascribed to this tool³².

Across all three legal systems, impact assessment has a shared purpose: to provide a concrete analytical process capable of evaluating how AI may affect the fundamental values and rights safeguarded within each legal system, and to establish measures to prevent irreversible harms. Nevertheless, a closer comparative examination reveals notable distinctions among the frameworks, which are crucial for understanding both the potential and the limitations of impact assessment as a mechanism mainly aimed at protecting people's fundamental rights³³.

In Canada, the main piece of legislation to be examined is the Canadian Directive on Automated Decision-Making of 2019, which provides the most comprehensive and detailed model of impact assessment. The Directive, applicable to situations in which AI is employed to make or support administrative decisions by federal institutions, assigns a central role to impact assessment within its regulatory framework³⁴. The type and level of impact generated by the use of AI systems are parameters for determining the applicability of the general obligations and safeguards prescribed by the Directive³⁵. Several of the guarantees and obligations contained in the Directive are, in fact, implemented in more detailed and stringent forms as the AI

blico comparato ed europeo», Special issue (2024), p. 979 ff.; G. Smorto, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in «DPCE online», 1 (2023), p. 339 ff.

³² On the importance of identifying case studies, according to various methodological criteria, in comparative public law analysis cfr. R. Hirschl, *The Questions of Case Selection in Comparative Constitutional Law*, in «The American Journal of Comparative Law», 1 (2005), p. 125 ff.

³³ E. Öricü, *Methodologies for Comparative Law*, in J.M. Smits, J. Husa, C. Valcke, M. Narciso (eds), *Elgar Encyclopedia of Comparative Law*, Edward Elgar Publishing, Cheltenham 2023, pp. 42-50.

³⁴ Art. 5, Directive on Automated Decision-Making. For a general comment on the Canadian Directive cfr. T. Scassa, *Administrative Law and the Governance of Automated Decision Making: A Critical Look at Canada's Directive on Automated Decision Making*, in «U.B.C. Law Review», 54 (2021), p. 251 ff.; B. Attard-Frost, A. Brandusescu, K. Lyons, *The governance of artificial intelligence in Canada: finding and opportunities from review of 84 AI governance initiatives*, in «Government Information Quarterly», 2 (2024), pp. 1-24.

³⁵ Appendix C, *Directive on Automated Decision-Making*.

level of impact increases, and consequently, as the risks to the protection of fundamental rights intensify. From this perspective, the Canadian model of impact assessment is particularly robust, as it explicitly provides for the adoption of specific measures designed to eliminate, or at least mitigate, the adverse effects that AI systems may have on the fundamental rights and values the Directive seeks to protect³⁶.

Further indicators of the completeness and coherence of the Canadian approach emerge from two key aspects: the identification of the protected legal interests upon which the impact of AI must be assessed, and the definition of graduated levels of impact that may result from its use. Regarding the first aspect, the Directive extends guarantees and protections to the rights of both individuals and communities, paying particular attention on safeguarding equality, dignity, privacy, autonomy, health, and well-being, as well as the economic interests of affected persons and the sustainability of the ecosystems within which AI systems are deployed. As to the second profile, the Directive distinguishes four levels of impact, classified according to the degree of reversibility of the effects produced and the temporal duration of those effects in relation to the protected interests at stake³⁷.

The overall effectiveness and precision of the Canadian impact assessment framework are further reinforced by another element. Indeed, the Canadian Government has issued a set of supplementary guidelines clarifying the application of the Directive and delineating the substantive scope of the parameters discussed above³⁸. More precisely, the Canadian Government specifies the areas of risk that may be relevant to the life cycle and use of AI systems, as well as some of the possible mitigating measures and the percentage score ranges that correspond to different levels of impact. Moreover, the Government also makes a questionnaire available to support interested parties in carrying out this algorithmic impact assessment³⁹.

In contrast, the United States legal framework exhibits notable differ-

³⁶ M. Karanicolas, *To Err is Human, to Audit Divine: A Critical Assessment of Canada's AI Directive*, in «Journal of Parliamentary and Political Law», 14 (2019), p. 1 ff.

³⁷ Appendix B, *Directive on Automated Decision-Making*. On these profiles see also H.L. Janssen, *An approach for a fundamental rights impact assessment to automated decision-making*, in «International Data Privacy Law», 1 (2020), pp. 76-106.

³⁸ Government of Canada, *Algorithmic Impact Assessment tool*, available at <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html#toc2>.

³⁹ Cfr. B. Deshaies, D. Hall, *Responsible use of automated decision systems in the federal government*, 1 December 2021, at <https://www.statcan.gc.ca/en/data-science/network/automated-systems>.

ences from the Canadian approach, being characterized by a comparatively lower degree of precision and detail concerning both the substantive content and procedural implementation of the impact assessment mechanism.

Even though the regulatory landscape in the field of AI is relatively fragmented and has recently undergone a significant shift in the federal approach to AI governance⁴⁰, the relevance of impact assessment tools in AI regulation has been acknowledged at federal level, especially by the Federal Artificial Intelligence Risk Management Act. This Act, within a framework primarily focused on the identification and mitigation of AI-related risks, emphasizes the need for federal agencies to consider the potential impact of artificial intelligence on legally protected interests. Specifically, the Act entrusts the National Institute of Standards and Technology (NIST) with the task of developing guidelines to assist federal agencies in implementing mechanisms for assessing and managing the risks associated with AI systems, with explicit attention to the possible implications for individual rights⁴¹. Within these NIST guidelines, the inclusion of an impact assessment mechanism forms part of the broader set of risk mitigation measures to be adopted by federal agencies. However, the regulatory framework does not provide detailed specifications regarding the parameters, criteria, or procedures governing the implementation of such assessments. Rather, the guidelines merely outline a general requirement to prioritize risk management according to the level of the impact produced, and to allocate appropriate resources for mitigation, without specifying anything on the nature of the potential impacts, the evaluative benchmarks to be applied, or the concrete measures to be implemented in proportion to the identified risks⁴².

At the State level, instead, the impact assessment receives somewhat greater emphasis, particularly in the regulatory approach adopted by the State of Colorado through the adoption and implementation of the Colorado Act concerning consumer protections in interactions with artificial intelligence systems of 2024. Under this statute, the impact assessment obligation

⁴⁰ C. Novelli, A. Gaur, L. Floridi, *Two Future of AI Regulation under the Trump Administration*, 24 April 2025, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5198926; V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer*, in «DPCE online», 1 (2025), pp. 49-65.

⁴¹ Section 2 (b) (2), H.R. 6936 - Federal Artificial Intelligence Risk Management Act of 2024.

⁴² National Institute of Standards and Technology, *Artificial intelligence Risk Management Framework (AI RMF 1.0)*, January 2023, at <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

consists primarily of the annual provision and retention by AI deployers⁴³ of technical documentation certifying: the intended purpose and objectives of the technology, its anticipated benefits, the data used and generated by the system, the performance evaluation metrics employed, and the transparency and post-deployment monitoring measures adopted by the deployer⁴⁴. Nevertheless, the Colorado Act does not establish a classification of impact levels based on the consequences of AI use, nor does it provide a comprehensive list of the rights and values that must be considered within the assessment. The only exception is the explicit reference to the principle of equality, as the Act requires deployers to examine the potential risk of discrimination arising from the functioning of AI systems⁴⁵. Furthermore, the Colorado Act does not mandate the adoption of specific or binding mitigation measures to limit or prevent risks or harms associated with AI deployment.

From this perspective, both the federal and state-level frameworks in the United States display a comparatively lower degree of regulatory precision than the Canadian legal approach, thereby leaving considerable discretion to the public authorities and private actors responsible for conducting impact assessments, including the definition of the relevant parameters and of the degree of AI impact on the protected interests and rights.

3.1. *Impact assessment mechanisms in the regulation of artificial intelligence. The fundamental rights impact assessment under the AI Act legal framework*

A similar framework for impact assessment to that provided by the US legal system, both at federal and state level, can also be identified within the regulatory framework developed by the European Union through the adoption of the Regulation (EU) 2024/1689 of the European Parliament and of the Council of

⁴³ Under the Colorado Act, a deployer is defined as a person who uses an AI system considered high-risk for professional purposes, as established by Section 6-1-1701 (6), SB 24-205 Concerning consumer Protections in interactions with artificial intelligence systems. According to this definition, therefore, a person who uses an artificial intelligence system for purely personal reasons cannot be classified as a deployer and, consequently, the provisions of the Colorado Act will not apply to them.

⁴⁴ Section 6-1-1703 (II) (b), SB 24-205 Concerning consumer Protections in interactions with artificial intelligence systems.

⁴⁵ Section 6-1-1703 (II) (b) (II), SB 24-205 Concerning consumer Protections in interactions with artificial intelligence systems. For a comment see R. Dotan, *US regulation of artificial intelligence*, in C. Lütge *et al.* (eds), *The Elgar Companion to Applied AI Ethics*, Edward Elgar Publishing, Cheltenham 2024, p. 153 ff.

13 June 2024, laying down harmonized rules on artificial intelligence (commonly referred to as AI Act). Regulation (EU) 2024/1689, indeed, introduces the obligation to carry out a fundamental rights impact assessment (FRIA) for AI systems, however this obligation applies only under specific and narrowly defined conditions. First, the impact assessment is required only for AI systems classified as high risk in accordance with Article 6(2) of the Regulation, thereby excluding other categories of high-risk systems also recognised under the AI Act⁴⁶. According to Article 27(1) of Regulation (EU) 2024/1689, all systems that are classified differently, or as high-risk systems under the provision of Annex I, are exempt from this mechanism⁴⁷. Moreover, AI Act expressly excludes from the impact assessment AI systems intended for use as safety components in the management or operation of critical digital infrastructure, road traffic, or the supply of water, gas, heating, or electricity⁴⁸. Second, the obligation to carry out an impact assessment is limited to specific categories of deployers explicitly identified by the Regulation⁴⁹. Accordingly, only public sector entities, private bodies providing public services, and deployers of high-risk systems used to assess individuals' creditworthiness or their eligibility for health and life insurance are subject to this requirement. All other users of high-risk systems falling outside these categories are exempt from this obligation⁵⁰. With regard to the content and implementation of the impact assessment, Regulation (EU) No. 2024/1689 provides that the process must include: a description of the processes in which the deployer intends to use the technology; a description of the period of time during which the system is expected to be used; the categories of individuals and groups potentially affected by the AI system in a specific context and the associated risks; a description of human oversight measures implemented; and the mitigation measures to be taken if the identified risks arise⁵¹. Furthermore, concerning

⁴⁶ In general, on the content and scope of the impact assessment provided for in the AI Act, see F. Palmioto, *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, in «European Journal of Risk Regulation», 17 January 2025, pp. 1-24.

⁴⁷ Systems not covered by this assessment mechanism would include, for example, medical devices incorporating artificial intelligence models.

⁴⁸ Article 27(1) of Regulation (EU) 2024/1689.

⁴⁹ Like the Colorado Act, the AI Act also identifies the deployer as «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», as defined in Article 3(4) of Regulation (EU) 2024/1689.

⁵⁰ Article 27(1) of Regulation (EU) 2024/1689.

⁵¹ Article 27(1)(a), (b), (c), (d), (e), (f), Regulation (EU) 2024/1689. For a commentary on this fundamental rights impact assessment see P.G. Chiara, F. Galli, *op. cit.*, p. 86 ff.; A. Mantelero,

the definition of the rights and values to be protected and against which the impact produced is to be measured, the European legislator identifies them in the general category of fundamental rights protected by the EU, especially those provided by the Charter of Fundamental Right of the European Union.

The AI Act provides also further information for the implementation of the fundamental rights impact assessment. It is mandatory only for the first use of the high-risk system, allowing deployers to rely, in similar cases, on previously performed impact assessment or existing impact assessment carried out by provider. If the deployer considers that, during the use of the high-risk system, one of the assessment elements has changed, the deployer shall intervene in order to update the information⁵². Moreover, where any of the obligations required for the implementation of the FRIA have already been fulfilled by carrying out the data protection impact assessment (DPIA), the fundamental rights impact assessment shall complement the latter evaluation⁵³. Finally, the deployer has also the duty to notify the market surveillance authority of the impact assessment results through the submission of a specific template that the AI Office will develop to help deployers in complying with this AI Act obligation⁵⁴.

4. *The fundamental rights impact assessment in the field of artificial intelligence. Lights and shadows in EU regulation and potential future paths*

The comparative reconstruction of the legal frameworks governing impact assessment provides an opportunity to draw several preliminary conclusions regarding the actual scope and effectiveness of this mechanism as a mean of protecting fundamental rights under the Regulation (EU) No. 2024/1689.

As previously emphasized, the implementation of impact assessment in the examined regulatory context is essential to make more substantive both processes of risks identification and balancing the rights at stake. First, the fundamental rights impact assessment allows to evaluate the concrete effects of deploying AI in a specific context of use and, consequently, better

The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template, cit., p. 7 ff.; C. Novelli, *The European Artificial Intelligence Act: some implementation issues*, in «Federalismi.it», 2 (2024), p. 110 ff.

⁵² Article 27(2) of Regulation (EU) 2024/1689.

⁵³ Article 27(4) of Regulation (EU) 2024/1689.

⁵⁴ Article 27(3) and (5) of Regulation (EU) 2024/1689.

define the meaningful risks to address. Thus, this tool contributes to make the AI Act's horizontal approach more adaptable to the needs that may arise depending on the sector in which the AI system is employed. Second, the substantial balancing carried out through the impact assessment mechanism may be the mean to achieve the main goals promoted by the AI Act. In this way, it is possible to foster AI development and use as long as its impact is under control and without compromising the protection of fundamental rights⁵⁵.

However, the analysis also highlights several structural weaknesses inherent in the current EU regulatory design of the fundamental rights impact assessment. In particular, the AI Act framework reveals significant shortcomings that limit the tool's potential to serve as an effective rights-protection mechanism. These weaknesses manifest in two principal ways: first, through the excessive discretion granted to private actors in determining the methods and parameters of the assessment, and second, through the restricted scope of application of the obligation itself. The latter issue is particularly pronounced, where the requirement to conduct the impact assessment does not extend to all AI systems, nor even to all systems classified as high risk, and it is limited to a specific group of deployers. This selective applicability risks undermining the consistency and universality of fundamental rights protection across AI contexts⁵⁶.

Moreover, further elements may weaken the efficacy of impact assessment as framed by Regulation (EU) 2024/1689. The choice of referring to such a broad assessment parameter like the general category of fundamental rights may render the mechanism meaningless and devoid of content, especially if taking into account the complex multi-level system of codification and protection of fundamental rights at both EU and national level⁵⁷.

⁵⁵ C. Novelli, *op. cit.*, p. 110 ff.; C. Novelli *et al.*, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in «Digital Society», 13 (2024), pp. 1-29; A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template*, *cit.*, p. 4 ff.

⁵⁶ On the limitations of the described fundamental rights impact assessment model see also M. Lasek-Markey, L. Hogan, *Delivering on the promise of the fundamental rights impact assessments in the EU AI Act: intersectionality and vulnerability*, in «European Journal of Law and Technology», 2 (2025), pp. 1-23. Among Italian legal scholars cfr. F. Donati, *La protezione dei diritti fondamentali nel Regolamento sull'intelligenza artificiale*, in «Rivista AIC», 1 (2025), pp. 1-20.

⁵⁷ Recital 48 of Regulation (EU) 2024/1689 tries to exemplify the fundamental rights mainly affected by the use of AI systems that may be: the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, the right to non-discrimination, the right to education, consumer

Finally, the lack of independent scrutiny of the impact assessment's results by an external public authority may also be problematic, as it risks reducing the assessment to a mere procedural formality, no more than the completion of a checklist by the deployer.

From this perspective, the current EU configuration of impact assessment risks shifting the delicate activity of rights-balancing, traditionally exercised by public and institutional actors, into the almost exclusive domain of private entities. Such a shift could weaken one of the fundamental principles of contemporary constitutionalism: that the protection and limitation of power, including technological power, must remain under public oversight. Entrusting the assessment process entirely to private deployers, without adequate institutional safeguards, creates the danger of conflicts of interest that could distort the evaluation of impacts and compromise the mechanism's legitimacy and protective function⁵⁸.

To prevent such an outcome and to address the weaknesses inherent in the approach set out in the AI Act, a potential response is offered by the impact assessment model developed and adopted by the Council of Europe's Committee on Artificial Intelligence: the Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (also known as HUDERIA methodology). Although non-binding, the HUDERIA methodology provides a structured framework for impact assessment designed to safeguard human rights, democracy, and the rule of law, and may aid as a supporting tool for complying with both the obligations laid down in the Framework Convention on AI and those established by the AI Act⁵⁹. The HUDERIA methodology is intended for both public and private actors who are required to identify, assess, and manage the risks generated by AI, and it is grounded

protection, workers' rights, the rights of persons with disabilities, gender equality, intellectual property rights, the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence, and the right to good administration. On the topic cfr. M. Lasek-Markey, L. Hogan, *op. cit.*, pp. 1-23. On issues that may arise in a system of multi-level protection of fundamental rights see G.F. Ferrari, *I diritti nel costituzionalismo globale: luci e ombre*, Mucchi, Modena 2023, p. 8 ff.; R. Bin, *Critica della teoria dei diritti*, Franco Angeli, Milano 2018, p. 69 ff.; A. Ruggeri, *La tutela "multilivello" dei diritti fondamentali, tra esperienze di normazione e teorie costituzionali*, in «Politica del diritto», 3 (2007), pp. 317-346.

⁵⁸ C. Casonato, *L'intelligenza artificiale fra pubblico e privato: una sfida per il costituzionalismo (e per i costituzionalisti)*, in «Diritto pubblico comparato ed europeo», 1 (2025), pp. 5-13.

⁵⁹ Council of Europe, *HUDERIA: new tool to assess the impact of AI systems on human rights*, 2 December 2024, at <https://www.coe.int/en/web/portal/-/huderia-new-tool-to-assess-the-impact-of-ai-systems-on-human-rights>.

in a socio-technical approach that evaluates the impact of AI by considering the interconnectedness of technology, human decision-making, and social structures⁶⁰.

This impact assessment model is organized into four distinct phases. The first, the *context-based risk analysis*, entails conducting a preliminary assessment of the consequences of AI use, analysing risk factors, mapping potential impacts and determining possible risk levels, as well as performing a triage activity for the most high-risk AI systems. The second phase, the *stakeholder engagement process*, focuses on the involvement of individuals or groups affected by the application of AI and its potential impacts, with the aim of integrating the perspectives of those who will directly experience the effects of the technology and thereby gaining a better understanding of its potentially negative consequences. The third phase, dedicated more specifically to *risk and impact assessment*, involves carrying out the assessment in light of the two preceding phases, according to clearly defined criteria such as the scale of the impact, the number of people affected, the duration, reversibility, and probability of the impact. The final phase, the *mitigation plan*, requires identifying and designing mitigation measures according to a hierarchical criterion based on the severity and probability of the impact, as well as defining specific remedies for individuals who suffer adverse consequences from the application of AI.

The HUDERIA methodology also stipulates the need for ongoing monitoring and continuous review of the impact assessment, with reference to the factors relating to the development, deployment, and use of AI within real-world environments⁶¹.

The HUDERIA methodology, thus, offers an impact assessment model with a higher level of precision in the definition of the parameters of the assessment, of the criteria for the implementation of the mitigation measures and pays more attention on the specificity of the protected values, like for democracy and the rule of law. In these terms, the integration of the fundamental rights impact assessment model provided for in the AI Act with that

⁶⁰ It seems appropriate to highlight how the recognition of artificial intelligence as a socio-technical product would represent a fundamental step in the process of regulating it and limiting the powers attributable to this technology. In this regard, see S. Lindgren, *Introducing critical studies of artificial intelligence*, in S. Lindgren (ed.), *Handbook of Critical Studies of Artificial Intelligence*, Edward Elgar Publishing, Cheltenham 2023, pp. 1-19.

⁶¹ Council of Europe, *HUDERIA: new tool to assess the impact of AI systems on human rights*, 2 December 2024, at <https://www.coe.int/en/web/portal/-/huderia-new-tool-to-assess-the-impact-of-ai-systems-on-human-rights>.

outlined by the HUDERIA methodology would promote a more coherent and comprehensive framework for AI regulation.

Looking ahead, such complementation could enable the realization of a genuine co-regulatory model, one that reconciles the imperatives of technological innovation with the foundational goals of contemporary constitutionalism: the protection of fundamental rights, the preservation of human dignity, and the legitimate exercise of public authority over the transformative power of technology.

Abstract

This paper seeks to examine the role of impact assessment mechanisms as instruments for the protection of fundamental rights within the regulatory frameworks governing emerging technologies, with specific reference to artificial intelligence systems. It will first consider the increasing prominence of impact assessments as a governance tool for artificial intelligence, highlighting their dual function: on the one hand, to safeguard the diverse interests implicated in the deployment of intelligent systems, and on the other, to prevent undue limitations on the development and application of such technologies. Subsequently, the paper will analyse, from a comparative perspective, the design and implementation of impact assessment mechanisms in the field of artificial intelligence, with particular emphasis on the European Union framework under the AI Act.

Keywords: fundamental rights; artificial intelligence; impact assessment; comparative law; European Union.

Marta Fasan
University of Trento
marta.fasan@unitn.it