Normative Considerations on Impact Assessments in EU Digital Policy*

Pier Giorgio Chiara - Federico Galli

Abstract

This paper assesses the increased normative role of impact assessments in the EU digital governance. We first investigate how impact assessments have gained prominence as regulatory tools in regulating the digital dimension. Then, we analyse, also from a comparative perspective, three different impact assessment models enshrined in EU legal acts (i.e., the GDPR, the AI Act and the DSA). Finally, we highlight six shortcomings common to the previously addressed models.

Summary

Keyword

impact assessment – systemic risk assessment – data protection impact assessment – fundamental rights impact assessment – EU digital policy

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco". While the research results are based on a combined effort, Section 2 should be attributed to Pier Giorgio Chiara, while, Sections 1 and 3 to Federico Galli. Conclusions are shared reflections. Pier Giorgio Chiara was supported by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU. Federico Galli was partially supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (GA. 833647) and by the PRIN 2022 Project DAFNE (P2022R7RS9) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

1. Impact Assessments as Regulatory Tools

Impact assessment can be described as a systematic process for analysing the potential effects or consequences of particular actions, projects, policies, or decisions. In the field of regulation, impact assessments are studied from two different perspectives: i) as part of a policy-making process and ii) as a tool for regulation.

In the first case, impact assessments are procedures for regulators to gauge the various effects of policy-making initiatives before they are implemented. The primary purpose of these assessments is to provide a comprehensive understanding of the broader implications of proposed policies, allowing for informed decision-making[1]. For example, so-called "regulatory impact assessments" (RIAs) have surfaced as a critical tool for ensuring "better regulation"[2] and more evidence-based public policies.

In the second case, impact assessments are regulatory tools in which private or public entities account for the potential effects of their activities on various aspects, such as the environment, society, economy, or specific stakeholders. This article will deal with this second type of impact assessment.

The use of impact assessment as a regulatory tool took hold during the second part of the 20th century in the context of self-regulatory initiatives of virtuous organisations. For example, environmental impact assessments have gained prominence since the 1970s in industries with significant ecological footprints, ensuring that private entities operate environmentally responsibly[3]. Other impact assessments have emerged in the last decades[4], such as human rights impact assessments[5], health impact assessments[6], and privacy impact assessments[7].

As society has started to recognise the increasing impact of organisations on various facets of social life, from technology companies shaping digital landscapes to industries influencing environmental sustainability, impact assessments have been increasingly included in some top-down legislative measures. One of the earliest examples is Directive 2011/92/EU[8], which introduced the environmental impact assessment (EIA) process, which ensures that projects likely to have significant effects on the environment are subject to an assessment by their developer prior to their authorisation.

---

1 C. Kirkpatrick-D. Parker, *Regulatory Impact Assessment: Towards Better Regulation?*, Cheltenham-Northampton, 2007.

2 European Commission, *Better Regulation Guidelines SWD,* 2021, 305 final, , 10.

3 J. Glasson-R. Therivel, *Introduction to Environmental Impact Assessment*, London, 2013.

4 The International Association for Impact Assessment (IAIA) has played a crucial role in promoting and applying these assessments beyond their environmental origins.

5 G. De Beco, *Human Rights Impact Assessments,* in *Netherlands Quarterly of Human Rights*, 27, 2009, 139.

6 B. Harris-Roxas et al., *Health Impact Assessment: The State of the Art,* in *Impact assessment and project appraisal,* 12, 2009, 43.

7 D. Wright, *The State of the Art in Privacy Impact Assessment,* in *Computer Law & Security Review*, 28, 2012, 54.

8 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment, later amended by the Directive 2014/52/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment.

In these cases, impact assessments become the object of due diligence obligations, whose violations may result in sanctions enforced by the state through specialised authorities.

This development has led to new thinking of impact assessments as co-regulatory mechanisms[9]. Co-regulation is an interface between top-down regulation (i.e., hard law) and self-regulation (i.e., soft law), where the legislator «entrusts the attainment of specific policy objectives set out in legislation or other policy documents to parties which are recognised in the field (such as economic operators, social partners, non-governmental organisations, standardisation bodies or associations)»[10]. Accordingly, impact assessments are an instance of co-regulation, as they involve both regulators in setting overarching goals and detailing processes and the regulated entities in analysing and managing the impacts of their economic and social activities in relation to these goals and processes

Impact assessments as regulatory tools are also tightly intertwined with the notion of risk and a risk-based approach to regulation[11]. Risk is generally understood as the combination of the likelihood of an adverse outcome materialising (e.g., harm) and the potential severity of such harm. Impact assessments generally involve, but are not limited to, quantitatively assessing impact in terms of risk. Thus, the risk analysis is a key aspect of impact assessments. Also, as risk-based regulation is committed to constraining the behaviours of people and organisations only in a way proportional to the particular risk identified, impact assessments serve the risk-focused perspective, aiming to anticipate and mitigate potential harms before they occur. This interconnectedness underscores the role of impact assessments in promoting regulatory frameworks that are both evidence-based and responsive to potential risks.

Against this backdrop, this work outlines how "impact assessments as regulatory tools" have become increasingly popular in EU digital policy and regulation (Section 2). Moreover, it contributes to the existing literature on digital governance in the EU by i) providing a systematic overview of three main impact assessment models having a bearing on the development and use of digital products, services and applications in the EU (i.e., the GDPR's Data Protection Impact Assessment (DPIA); the Fundamental Rights Impact Assessment (FRIA) under the Artificial Intelligence Act; and the DSA's systemic risk assessment (SRA)); ii) mapping out some inherent limitations of impact assessments as regulatory instruments (which are increasingly adopted by EU policies) to the three previously analysed models (Section 3); iii) presenting possible solutions to overcome these hurdles. This study shall also serve as a baseline for future research, in particular, concerning the normative implications addressed in Section 3.

[9] R. Binns, *Data protection impact assessments: a meta-regulatory approach*, in *International Data Privacy Law*, 7(1), 2017, 22.

[10] European Commission, *Better Regulation Toolbox,* 2023, 124.

[11] J. B. Wiener, *Risk Regulation and Governance Institutions,* 2010, OECD report.

2. Impact Assessments in EU digital policy

Impact assessments have become a prominent regulatory tool in the current EU digital policy-making[12]. In this context, the EU has started mandating different entities' specific impact assessments in connection with the development of digital technologies. Some areas of EU law (i.e., privacy and data protection, artificial intelligence) explicitly introduce impact assessments as a requirement for its addressees, while other areas of EU digital regulation (i.e., cybersecurity, online platform services, banking and finance, children online protection, etc.) hinge on the somewhat vaguer paradigm of "risk management", which still is an *ex-ante* due diligence obligation. In any case, both instruments serve as a structured and systematic method to evaluate the implications of digital products and services before they become entrenched in the market and ensure that these can align with specific technical, legal and social goals relevant to the EU.

Specifically, a particular emphasis has recently been placed on fundamental rights and social values. In this context, risk-based impact assessments mandated on private actors take into consideration the goal of upholding fundamental rights and values enshrined in the Charter of Fundamental Rights of the European Union. This trend, which may deserve an analysis on its own, can be read as one of the many responses of "digital constitutionalism" contributing to the privatisation of fundamental rights protection[13]. Also, this movement is perfectly in line with increased pressure on private actors on a global and regional scale to align with human rights and social goals (see., e.g., corporate social responsibility)[14].

Three models of impact assessment[15], which consider fundamental rights and social interests as protected values, can be identified in three different EU legal regulations in the digital field: (1) the data protection impact assessment (DPIA) set out in Art. 35 GDPR; (2) the fundamental rights impact assessment (FRIA) established at Art. 27 of the approved Artificial Intelligence Act; and (3) the systemic risk assessment (SRA) obligations for Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) set out in Arts. 34-35 of the Digital Services Act.

---

[12] A. Calvi-D. Kotzinos, *Enhancing AI Fairness Through Impact Assessment in the European Union: A Legal and Computer Science Perspective*, in *Proceedings of the 2023 ACM conference on fairness, accountability, and transparency*, 2023.

[13] See, among others, E. Celeste, *Digital constitutionalism: a new systematic theorization*, in *International Review of Law, Computers & Technology*, 33(1), 2019, 76 and, more extensively, G. De Gregorio, *Digital Constitutionalism in Europe, Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022.

[14] See, recently on this, P. Balboni-K. Francis, *Data Protection as a Corporate Social Responsibility*, Cheltenham-Northampton, 2023.

[15] Following Mantelero, for the purpose of the article we cluster the DSA's "systemic risk assessment" requirement under the broader, functional definition of "impact assessment" given above. Cf. A. Mantelero, *Fundamental rights impact assessments in the DSA*, in *Verfassungsblog: On Matters Constitutional*, 2022.

2.1. GDPR: the Data Protection Impact Assessment (DPIA)

The GDPR establishes the principle of accountability (Art. 5(2) GDPR), according to which data controllers shall be able to prove compliance with the principles of personal data protection enshrined in Art. 5(1) GDPR (lawfulness, fairness and transparency; data minimisation; accuracy; purpose limitation; storage limitation; integrity and confidentiality). The accountability principle builds on a risk-based approach[16], i.e. the degree of expected compliance is determined by the inherent risk of the overall personal data processing operations. The risk-based approach is rooted in Art. 25(1) GDPR, as data controllers are required to implement appropriate technical and organisational measures, considering the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the *risks* of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. Therefore, the GDPR introduces a high-level legal standard (i.e., compliance with personal data protection principles) without setting how such a standard can be implemented in practice, as the spirit of accountability ultimately requires the data controllers to ascertain the risk of data processing and determining appropriate measures to mitigate such risk[17].

The accountability principle and risk-based approach are further exemplified by Art. 35 GDPR[18], for it introduces an obligation for data controllers to perform a "data protection impact assessment" (DPIA) prior to processing that is likely to result in a high risk to the rights and freedoms of natural persons, especially if new technologies are involved[19]. The GDPR contextual risk-based approach is also reflected in this provision, as data controllers must adapt their compliance efforts to the actual (high) risks posed by their processing operations. Once the DPIA is completed, if the residual risk to the rights and freedoms is (still) high, only then will data controllers consult the supervisory authority[20]. This is a further example of the accountability principle and the paradigm shift from the 95 Data Protection Directive, where authorities were tasked to preventively assess processing operations likely to present specific risks to the rights and freedoms of data subjects (sc. prior checking)[21].

Concerning the DPIA, Paragraphs 3-5 of Art. 35 GDPR are preoccupied with determining when a DPIA is required or not. In this regard, Article 29 Working Party clustered specific processing operations that require a DPIA due to their inherent high

16 R. Gellert, *Understanding the notion of risk in the General Data Protection Regulation,* in *Computer Law & Security Review;* 34, 2018, 2.

17 U. Pagallo-P. Casanovas-R. Madelin, *The Middle-Out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data*, in *The Theory and Practice of Legislation,* 7(1), 2019, 10.

18 A. Christofi et al., *Erosion by Standardisation: Is ISO/IEC 29134: 2017 on Privacy Impact Assessment up to (GDPR) Standard?*, in *Personal data protection and legal developments in the European Union*, 2020, IGI Global, 1796.

19 Art. 35(1), GDPR.

20 Art. 36(1), GDPR.

21 Art. 20, Directive 95/46/EC.

risk into nine criteria, which are outcomes-based: 1) evaluation or scoring; 2) automated decision-making with legal or similar significant effect; 3) systematic monitoring; 4) sensitive data or data of highly personal nature; 5) data processed on a large scale; 6) matching or combining datasets; 7) data concerning vulnerable data subjects; 8) innovative use or applying new technological or organisational solutions[22]; 9) when the processing in itself "prevents data subjects from exercising a right or using a service or a contract"[23].

Paragraph 7 of Art. 35 GDPR puts forward a minimum list of elements that a DPIA has to include: a) a systematic description of the envisaged processing operations and the purposes of the processing; b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c) an assessment of the risks to the rights and freedoms of data subjects; and d) the measures envisaged to address the risks. The controller shall seek the views of data subjects or their representatives on the intended processing (Art. 35(9) GDPR) and constantly monitor whether the processing is performed in accordance with the DPIA (Art. 35(11) GDPR).

Yet, if we turn our attention to widely adopted DPIA methodologies (e.g., the model designed by the French Data Protection Authority, the CNIL[24]), risk assessments only sometimes embrace the full scope of Art. 35(7)(c) GDPR. In particular, the "risk to rights" reference is often neglected as DPIA models are still primarily centred on risks to privacy and data protection, i.e. data security, mirroring the approach of the Privacy Impact Assessments (PIA)[25] under the previous Data Protection Directive: «despite specific references in the GDPR to the safeguarding of rights and freedoms in general as well as to societal issues, the new assessment models do nothing to pay greater attention to the societal consequences than the existing PIAs»[26]. Rather, GDPR's risk management process, that is, the DPIA, would require data controllers to assess processing's impacts vis-à-vis the full catalogue of EU fundamental rights, i.e. the Charter of Fundamental Rights of the EU[27].

---

[22] For example, the processing of personal data by AI providers and deployers would require a DPIA pursuant to several of the above-mentioned criteria. In certain cases, the development and use of AI systems may require data processing at a large scale (n. 5) or entail the evaluation of personal characteristics (n. 2), if not automated decision-making (n. 2). In any case, AI technologies may constitute at the state of the art an "innovative technological solution", thus requiring a DPIA under the criterion n. 8.

[23] Art. 29 WP, *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*, 9-11.

[24] CNIL, *Privacy Impact Assessment (PIA) Methodology*.

[25] Art. 20, Directive 95/46/EC.

[26] A. Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*, 2022, London-New York, 23.

[27] D. Hallinan-N. Martin, *Fundamental Rights, the Normative Keystone of DPIA*, in *European Data Protection Law Review*, 6(2), 2020, 178; E. Kosta, *Article 35 Data Protection Impact Assessment*, in C. Kuner-L. A. Bygrave-C. Docksey-L. Drechsler (eds.) *The EU general data protection regulation: A commentary,* Oxford, 2020, 671.

2.2. AI Act: The Fundamental Rights Impact Assessment (FRIA)

On 13 March 2023, the European Parliament passed the AI Act (AIA), laying down harmonised rules on artificial intelligence in the EU. The AI Act bridges the "traditional" risk-based approach of "EU digital law" with an enhanced product safety approach, for it is hybridised with a "rights-based approach"[28]. In particular, the "risk-based approach" is declined in the AI Act in a different fashion from the GDPR, as it determines the regulatory burdens for AI operators based on the risk entailed by specific categories of AI systems and AI use cases to safety, health, and fundamental rights. AI systems are clustered into four pre-determined risk categories, i.e., unacceptable, high, low, and minimal and are covered by corresponding regulatory measures[29]. The Regulation mainly establishes rules for high-risk AI systems, among which essential requirements and due diligence obligations are distributed among developers and deployers. Developers must ensure the application of essential requirements and undergo the relevant conformity assessment. Deployers are instead bound to use the AI systems according to instructions given by the provider and, importantly, carry out a fundamental right impact assessment (FRIA).

In particular, the obligation of the deployer to perform a FRIA prior to deploying a high-risk AI system into use is contained in Art. 27 of the AI Act. Three categories of actors linked to high-risk AI systems are in scope: i) deployers that are bodies governed by public law; ii) private operators[30] providing public services (e.g., education, healthcare, social services, housing, administration of justice); and, iii) operators deploying high-risk systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score and intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance. The assessment shall include at least: a) a description of the deployer's processes where the high-risk AI system will operate; b) the period of time and frequency of the system's use; c) the categories of persons and groups likely to be affected by the use of the system; d) the specific risks of harm likely to impact the previously identified persons; e) a description of the implementation of human oversight measures; f) the measures to be taken in case of the materialisation of these risks. Following to a dynamic risk-based approach, subject to changes in the above-mentioned factors, deployers have to update the FRIA accordingly[31]. Upon finishing the impact assessment, deployers are required to notify the market surveillance authority of the results of the

[28] T. Evas, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI,* in *AIRe – Journal of AI Law and Regulation*, 1(1), 2024, 98-100. See also M. Almada and N. Petit, *The EU AI Act: Between product safety and fundamental rights,* 2023, *Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59*, available at *SSRN*.

[29] C. Novelli et al., *Taking AI Risks Seriously: A New Assessment Model for the AI Act,* in *AI & Society*, 2023, 1.

[30] Art. 3(8), AI Act: "operator" means the provider, the product manufacturer, the deployer, the authorised representative, the importer or the distributor.

[31] Art. 27(2), AI Act.

assessment[32].

It may be the case that deployers required to conduct a FRIA have already carried out a DPIA pursuant to Art. 35 GDPR. In fact, data protection rules, including the obligation to carry out a DPIA, apply in the context of AI use as long as personal data are processed.[33] This is all the more true given the broad understanding of the "personal data" concept pursuant to Art. 4(1) GDPR and relevant case law.[34] Moreover, using an AI system may constitute a decision based solely on automated processing, including profiling, as in Art. 22 GDPR.

If any of the elements of the FRIA are already met through the DPIA pursuant to the GDPR (or the LED Directive[35]), Art. 27(4) of the AI Act establishes that a FRIA should be conducted in conjunction with such instruments. The importance of this provision should not be underestimated, for it entails two significant normative consequences. From an operational perspective, the legal text seems to have already clarified the relationship between the two instruments (i.e., the DPIA and the FRIA) with a view to avoiding seemingly duplicative requirements that might have created a burden for economic operators. Moreover, from a strict legal perspective, including such FRIA in the AIA would have entailed, among other things, a "downscaling" of the right to data protection, which, in the absence of (more) comprehensive legal answers, has been assigned with the GDPR, and specifically Art. 35, a safeguarding role for the entire catalogue of fundamental rights – as seen above.

The final version of the FRIA obligation differs significantly from the original European Parliament (EP) proposal. First, the EP draft provision would have applied to all deployers of high-risk AI systems. Second, several important elements originally included in the FRIA are now missing: an outline of the intended geographic scope of the system's use; the reasonably foreseeable impact on fundamental rights, as well as on the environment; and a detailed plan describing the measures or tools that will help mitigate the identified risks. In particular, absent a risk mitigation plan, the deployer should have refrained from putting the high-risk AI system into use and informed the provider as well as the national supervisory authority without undue delay (Art. 29a(2) EP draft AIA). Third, similar to Art. 35(9) GDPR, according to the EP's FRIA model, deployers (except for SMEs) would have involved representatives of the persons or groups likely to be affected by the system (Art. 29a(4) EP draft AIA). The EP found it appropriate to list a number of stakeholders (i.e., equality bodies, consumer and data

[32] There is however an exception to notify for "exceptional reasons of public security": see Amnesty International, *EU's AI Act fails to set gold standard for human rights,* April 2024, 3.

[33] European Data Protection Authorities have been producing guidelines and recommendations on the development and implementation of artificial intelligence systems that are GDPR-compliant as early as the entry into application of the Regulation. For example, see the report from the Norwegian Supervisory Authority, *Artificial Intelligence and Privacy,* 2018; more recently, the French SA started publishing several dedicated resources on AI.

[34] E.g., CJEU C-582/14, *Breyer* (2016), ECLI:EU:C:2016:779.

[35] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. It is worth noting that the interplay between the LED and the incoming AI Act will be relevant.

protection agencies, and social partners) as well as to include a deadline (i.e., six weeks) to obtain a response from them. Finally, deployers who are public authorities would have been mandated to publish a summary of the impact assessment – an element missing from the corresponding Art. 35 GDPR (Art. 29a (5) EP draft AIA)[36].

On a different note, one may wonder whether Art. 27 AIA is the only provision of the Regulation imposing a risk or impact assessment to fundamental rights[37]. Art. 9, establishing a risk-management system as an essential requirement for high-risk AI systems, also stresses the need to identify and analyse the known and reasonably foreseeable risks that the high-risk AI system can pose to health, safety and *fundamental rights*. The developer of a high-risk AI system is competent in ensuring the application of essential requirements. Thus, the developer must also ensure that the risks stemming from AI systems are identified, analysed, and mitigated, considering the risks to fundamental rights[38].

However, the risk assessment contained in Art. 9 differs from Art. 27 FRIA both in terms of rationale and scope. First, the fundamental rights risk assessment under Art. 9 FRIA is a requirement for all high-risk AI systems, contrary to the limited scope of Art 27. Second, Art. 9 requirements must be implemented by providers and not deployers. Third, in line with the new legislative framework (NLF) principles and architecture, providers may comply with mandatory essential requirements (e.g., Art. 9 AIA) by applying harmonised technical standards (which is voluntary)[39].

Whether the two fundamental rights assessments may influence each other, we claim that this occurrence is almost inevitable due to the inherent information asymmetry between the provider and the deployer. Providers possess key knowledge about system properties and technical limitations, impacting risk assessments during deployment. Thus, in the FRIA, deployers should consider information outlined in Art. 13[40]. Deployers may also rely on existing assessments from providers, tailoring their own assessments according to the system's use. On the other hand, deployers, being closer to usage contexts, understand individual and group risks better and are obligated to promptly notify providers of any emerging risks or incidents. This empowers providers to update risk management systems to address newly identified risks for fundamental rights.

The above-mentioned differences between providers and deployers lead to a signif-

[36] E. Kosta, *Article 35 Data Protection Impact Assessment*, cit., 675.

[37] A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template,* in *SSRN Electronic Journal*, 2024.

[38] Art. 9(2)(a), AI Act.

[39] European Commission, *COMMISSION NOTICE - The 'Blue Guide' on the implementation of EU product rules 2022,* 2022/C 247/01.

[40] The information that the provider must give to the deployer pursuant to Art. 13 AI Act is extremely relevant for conducting a FRIA, as it includes the characteristics, capabilities, and limitations of the high-risk AI system, including its intended purpose and level of accuracy, robustness, and cybersecurity metrics; any foreseeable circumstances that may impact accuracy, risks to health and safety, or fundamental rights must be disclosed; the technical capabilities to provide relevant information, performance regarding specific users or groups, and specifications for input data should be provided where appropriate; information to interpret and use the system's output effectively, predetermined changes, and human oversight measures must also be outlined etc.

icant implication with regard to the effectiveness of the two FR-related obligations. As we will see later in Section 3, these assessments, in order to be meaningful, must necessarily be context-dependent. In this regard, deployers are best placed to properly assess the risks posed to specific rights by the system in a given context and balance the competing interests at stake.

2.3. DSA: The Systemic Risk Assessment (SRA)

The Digital Services Act[41] (DSA) is part of a broader policy strategy of the EU Commission[42] that aims to develop a legal framework to protect users' fundamental rights online without hampering business expansion[43].

The DSA applies to intermediary service providers[44] who offer their services to recipients located in the Union (Art. 2(1) DSA). The Regulation adopts a scalable approach to the duties imposed on internet service providers: due diligence obligations, supervision, and sanctions are tailored to the type, size and nature of the provider concerned. Accordingly, the DSA sets out "basic" obligations applicable to all intermediary service providers (Arts. 11-15 DSA); additional obligations for hosting service providers, including online platforms (Arts. 16-18 DSA); additional provisions for providers of online platforms (Arts. 19-32 DSA); finally, additional obligations for providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) (Arts. 33-43 DSA).

In the last regulatory layer, the DSA introduces the obligation to carry out a systemic risk assessment (SRA). VLOPs and VLOSEs are required to identify and assess systemic risk «stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services» (Art. 34(1) DSA). Such a risk assessment is conceived as dynamic in nature, as the providers have to carry out such assessment once designated as VLOPs and VLOSEs by the Commission and at least once a year (Art. 34(1) DSA).

Notably, the SRA includes not merely the modalities of service provision but also the use of "algorithmic systems". Therefore, whereas the SRA does not explicitly deal with AI, it will likely influence the design and use of AI systems commonly used by online platforms to provide their service (e.g., recommender systems, content moder-

[41] Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC.

[42] European Commission, *Shaping Europe's Digital Future*, 2020. In particular, The Digital Services Act package, implementing the Strategy, includes two regulations: the Digital Services Act (DSA) and the Digital Markets Act (DMA).

[43] A. Turillazzi et al., *The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications,* in *Law, Innovation and Technology*, 15, 2023, 83.

[44] Under Art. 3 DSA, intermediary services consist of mere conduit services, caching, and hosting services. Online platforms, such as social networks or online marketplaces, fall into the category of hosting services, although they not only store information provided by service recipients but also disseminate this information to the public at their request.

ation, online advertising)[45]. The AI Act's FRIA is, therefore, not the only risk assessment required in the context of AI. It is, however, unlikely that a SRA and a FRIA will have to be carried out together, since the use cases of high-risk systems under the AI Act requiring a FRIA do not include the systems used by the platforms covered by the DSA requiring a SRA [46].

The risk assessment shall take into account four categories of risks defined as "systemic": i) the dissemination of illegal content; ii) any actual/foreseeable negative effects on fundamental rights, including dignity, private life and data protection, freedom of expression, non-discrimination, respect for rights of children and high level of consumer protection; iii) any actual/foreseeable negative effects on civic discourse and electoral processes as well as public security; iv) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

Like the FRIA and DPIA, the SRA includes considerations around the impact on fundamental rights. In this regard, scholars have noted that Art. 34(1)(b) only requires providers to assess related negative effects to fundamental rights instead of directly targeting infringements[47]. However, in terms of scope, the SRA is limited to specific rights, which are supposed to most likely be at risk in online platform environments. At the same time, SRA's scope is remarkably larger, as it encompasses interests that are beyond the protection of individual rights and covers important economic and social interests, such as consumer protection, public health and gender-based violence.

Albeit not yet mature, there is some experience in assessing "negative effects", or impacts, on fundamental rights. Assessing the negative effect on civic discourse, electoral processes, and public security is another issue[48]. The fact that VLOPs and VLOSEs are multi-national actors operating in different markets and jurisdictions might complicate such assessments even further.

The last category of systemic risks presents a different set of problems since it brings together «different situations relating to subjective status (minors), conduct (gender-based violence), collective (public health) and individual interests (physical and

[45] Arguably, all these systems are included in the definition of "AI system" given in the AI Act («a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments»). Cf., e.g., with definition of "recommender system" contained in Art. 3(s) DSA.

[46] The European Parliament had introduced an amendment to Annex III of the AI Act, which included recommender systems used by VLOPs and VLOSEs in the list of high-risk AI systems. However, the amendment did not make it into the political agreement and the approved text. In our view, the only potential overlap is confined the possibility of considering recommender systems as "AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda", pursuant Annex III, Point 8, lit. b) of the AI Act.

[47] A. Turillazzi et al., *The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications*, cit., 96.

[48] See N. Eder, *Making systemic risk assessments work: How the DSA creates a virtuous loop to address the societal harms of content moderation,* in *SSRN Electronic Journal*, 2023, 8-9.

mental well-being)»[49]. The regulatory decision of narrowing the assessment down to specific (and diverse) risk categories, coming at the expense of a more general and flexible framework, could backfire in the long run as situations worth protecting might fall outside the scope of the instrument, irrespective of any future amendments to the legal text to ensure futureproofing.

Art. 35 DSA contains a non-exhaustive list of mitigation measures that providers of VLOPs and VLOSEs must put in place, provided that they are reasonable, proportionate, effective and tailored to the specific systemic risks identified. The mitigation measures cover the overall "techno-legal architecture" of the service, as they include not only adapting and testing the algorithmic systems (e.g. content moderation systems, recommender systems, and advertising systems) and interfaces but also modifying platforms' terms and conditions and enforcement procedures to align them with evolving legal standards and community expectations.

As in the case of the GDPR's DPIA and the AIA's FRIA, DSA's risk assessment is also context-based, answering to a risk-based logic. Unlike the other two regulations, however, Art. 37 DSA requires that VLOPs' and VLOSEs' providers be subject, at their own expense and at least once a year, to independent audits to assess compliance with i) Chapter III obligations; and ii) any commitments undertaken pursuant to codes of conduct (Arts. 45-46 DSA) or crisis protocols (Art. 48 DSA).

Following a law & economics rationale, some scholars argued in favour of such risk management obligations as VLOPs and VLOSEs' providers «are often best placed to know the problems caused by their users and how to remedy them in the most cost-efficient way. Equally, it is understandable that the Commission wants the platforms themselves to bear the costs of inspecting compliance with the rules imposed by the DSA»[50].

Eventually, these risk management measures are showing their teeth, as confirmed by two formal proceedings opened by the Commission against TikTok in February[51] and April 2024[52], respectively. The latter, in particular, aims to inquire whether TikTok had carried out a diligent assessment of the risks (pursuant to Art. 34 DSA) and taken effective risk mitigating measures (pursuant to Art. 35 DSA) prior to the launch on the market of "TikTok Lite", especially with regard to the so-called "Task and Reward Program" of the app. The crux of the enforcement action lies in the likely adverse impacts of the "Task and Reward Lite Program" on the fundamental right to the person's physical and mental well-being, the respect of the rights of the child as well as its impact on radicalisation processes, as well as the lack of measures taken by TikTok to mitigate those risks. The Commission is empowered to take further enforcement actions, spanning from suspending the Program under investigation to non-compliance

[49] A. Mantelero, *Fundamental rights impact assessments in the DSA*, cit., 111.

[50] C. Cauffman-C. Goanta, *A New Order: The Digital Services Act and Consumer Protection*, in *European Journal of Risk Regulation*, 12, 2021, 770–771.

[51] European Commission, *Commission opens formal proceedings against TikTok under the Digital Services Act*, 19 February 2024.

[52] European Commission, *Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain and communicates its intention to suspend the reward programme in the EU*, 22 April 2024.

decisions, including administrative fines, should the infringement claims be proved.

3. Normative Considerations on Impact Assessments

In this section, we detail some considerations around the impact assessments models presented above. In particular, we group them around six shortcomings associated with impact assessments as effective tools to regulate the risk digital technologies poses on individuals and society.

3.1. Measuring Impacts

A significant hurdle in carrying out impact assessment is represented by the task of quantifying impacts.

This challenge particularly arises when impact assessments encompass fundamental rights and social interests[53]. This complexity relates to the incommensurability problem of fundamental rights, i.e. the impossibility of numerically determining the value scale of fundamental rights and the intensity of interference with them. According to Sampaio, "incommensurability is caused, in the constitutional domain, by the fact that fundamental rights (as well as the values they express) have an ultimate nature, so there are no criteria allowing them to be compared and, thus, to rationally determine which one should prevail"[54].

Besides fundamental rights and freedoms, those who have to carry out these impact assessments are confronted with the same hurdles when it comes to quantifying risks to, e.g., civic discourse, electoral processes and public security, as in the context of the DSA's systemic risk assessment. The intricate nature of these abstract concepts, which resist easy quantification due to their inherently subjective interpretation, is the root of the problem.

Even when one assumes that fundamental rights and other public fundamental interests (e.g., civic discourse) can be quantitatively measured[55], ascribing values to them requires interpretative reasoning and, ultimately, normative judgements. As known, fundamental rights are not merely correlative of duties and, similar to principles, do not translate in conduct to be directly applicable but still require argumentation, especially when competing principles are at stake. For example, the right to freedom of

[53] A. Rosga-M. L. Satterthwaite, *The Trust in Indicators: Measuring Human Rights*, in *Berkeley Journal of International Law,* 27, 2009, 253.

[54] J. S. Sampaio, *Proportionality: Measuring Impacts on Fundamental Rights*, in M. Seller-S. Kriste (eds.) *Encyclopedia of the Philosophy of Law and Social Philosophy*, 2019, London-New York, 2863, referring to the Robert Alexy's "Weighting Formula" for weighting fundamental rights in the act of balancing.

[55] For example, Sartor introduces the concept of "magnitude" to express the non-numerical quantitative reasoning and the possibility to use it in value-based reasoning, such as fundamental rights balancing. See G. Sartor, *The Logic of Proportionality: Reasoning with Non-Numerical Magnitudes,* in *German Law Journal,* 2012, 1419. On a different note, Mantelero also proposed a methodology to quantify impacts to fundamental and human rights in his Human Rights, Ethical, and Social Impact Assessment (HRESIA). See A. Mantelero, *Beyond Data: Human Rights, Ethical, and Social Impact Assessment in AI,* cit.

expression and information enshrined in Art. 11 of the Charter may appear straightforward in its content. Yet, its application in digital platforms presents intricate challenges. Consider the regulation of online content moderation on social media platforms. While individuals have the right to express themselves freely, the interpretation of this right in the context of combating hate speech and disinformation requires careful decisions on what content should be removed or allowed often to avoid harm to people. Upholding fundamental rights always requires an act of balancing, which in turn implies establishing the degree of satisfaction of a right and non-satisfaction of the competing right[56]. Such an evaluation, carried out by non-institutional actors such as platforms, is always subjective.

To address this inherent subjectivity, impact assessment models must be made explicit and contestable within the assessment framework. By doing so, individuals and institutions can engage in meaningful discourse regarding the assigned values and their implications. Striking a delicate balance between the quantitative and qualitative dimensions of fundamental rights and other societal interests is vital. The assessment process should navigate the intricacies of assigning values without oversimplifying the multifaceted nature of these concepts. This nuanced approach ensures a more comprehensive and accurate evaluation of the potential impacts of emerging digital technologies on fundamental rights and societal values, contributing to a more robust governance framework.

Coherently with its general, context-dependent approach – which finds one of its roots in the principle of accountability, Art. 35 GDPR is high-level; that is, it does not dictate to data controllers how to quantify impacts on data protection and fundamental rights. Thus, it is up to data controllers to develop a methodology for risk quantification and management which is adequate and proportionate to their specific personal data processing. Supervisory authorities, in this regard, provide meaningful guidance to data controllers by designing models that properly address the considerations expressed above 59, although the GDPR does not explicitly task SAs with this duty[57]. That being said, the burden of declining a general risk assessment model (risk evaluation, risk analysis, risk mitigation measures) in a given processing scenario rests on the data controller.

Whereas, in general, the AI Act acknowledges the need for further regulatory guidance (mainly from the Commission) to ensure coherence and effective application[58], Art. 27 of the AI Act largely follows the structure of Art. 35 GDPR[59]. Hence, the issues seen above also apply here. It is worth noting in this case that while Art. 27(5) mandating the AI Office to develop tools (i.e., a template for a questionnaire) to facilitate deployers in complying with their obligation to perform a FRIA is to be welcome,

[56] R. Alexy, *Constitutional rights, balancing, and rationality*, in *Ratio Juris*, 16, 2003, 131.

[57] According to Arts. 35 and 57 GDPR, SAs, in relation to assist data controllers in their duty to conduct a DPIA, only have to establish and maintain a list of the kind of processing operations which are subject to the requirement for a DPIA (Art. 35(4)).

[58] See T. Evas, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI,* cit., 101.

[59] This line of reasoning is also confirmed by the fact that Art. 27(4) AI Act acknowledges that several components of a FRIA can be already met through DPIA.

such questionnaire needs nevertheless to be integrated with sound and flexible (i.e., implementable in different contexts) methodologies for risk quantification and management, as seen above.
Unsurprisingly, also Art. 34 DSA does not contain indications for VLOPs' and VLOSEs' providers on how to quantify the systemic risks identified in the legal provision. One slight departure from the other two models, however, is the explicit mention of the two risk dimensions that every risk assessment shall take into consideration, namely severity and probability (Art. 34(1) DSA). Overall, the burden of designing a methodology to "diligently identify, analyse and assess" the systemic risks in the specific context of their services and proportionate to the risks faced rests on VLOPs and VLOSEs.

3.2. Effective Operationalisation

Related to the issue of quantifying impacts on fundament rights, another weakness of impact assessments is their effective operationalisation. Drawing lessons from the data protection field, impact assessments carried out by private actors risk resulting, in practice, in box-ticking exercises[60]. As a result, compliance may even be reached "on paper," but such a "standardised" one-fits-all approach fails to operationalise the (high-level) legal provision effectively. In this regard, every risk assessment - which is arguably the core aspect of an impact assessment - must confront the creation of risk indicators, the choice (which shall be subject to justification) of an appropriate risk matrix, and the selection of relevant risk dimensions (i.e., variables) as well as their combination[61].
Concerns about bureaucracy have also already been expressed by some scholars as well as industry, suggesting that mandatory impact assessments may entrench a command-and-control approach, undermining their intended purpose. It is generally recognised that rule-based, coercive, and punitive methods applied solely by regulators tend to lead to "ritualism" (following rules without understanding why they are there) and "creative compliance" (following the letter of the rules in such a way as to undermine their overall purpose, as in elaborate tax avoidance schemes). The fear is that mandatory impact assessments will focus more on demonstrating compliance with specific procedures rather than on flexible, substantive, and holistic risk assessment and mitigation.
Against this backdrop, all three impact assessments under GDPR, AI Act and DSA are equally affected by this shortcoming, for they ultimately share the same normative architecture.

[60] R. Gellert, *Understanding the notion of risk in the General Data Protection Regulation*, cit., 284; Art. 29 WP, *Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package*, 2013; A. Christofi et al., *Erosion by Standardisation: Is ISO/IEC 29134: 2017 on Privacy Impact Assessment up to (GDPR) Standard?*, cit., 1795.

[61] A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template,* cit., 24.

3.3. Interdisciplinarity

An effective operationalisation and implementation of private actors-led impact assessments, especially those having a bearing on fundamental rights and social interests, would necessarily require a multi-disciplinary team of experts, from lawyers and business managers to ethicists and engineers[62]. As already stressed throughout the paper, digital compliance - in particular in the EU - involves many different and complex legal texts. Multi-disciplinary teams of experts would best assist relevant stakeholders to contextualise high-level legal provisions in a given scenario with a view to providing a tailored application of legal and societal values of impact/risk assessment models.
We acknowledge, on the other hand, that this approach can create increased compliance costs for companies, especially for SMEs already struggling in a difficult economy[63]. Given that some players will lack resources for building a team of professionals with different expertise, EU competent authorities shall step up in terms of providing even more insightful guidance, e.g. via sector-specific and technology-specific assessments.
Regarding mandatory requirements, the three relevant legal texts are silent on this point. However, while the GDPR is completely silent on this account, the AI Act is generally keener on this perspective. With regard to the risk-management system requirement, Recital 65 suggests providers involve experts when identifying the most appropriate risk-management measures, and with specific regard to the FRIA, Recital 96 suggests deployers of high-risk AI systems include independent experts when collecting relevant information to perform the fundamental rights impact assessment. In this latter case, the (multidisciplinary) experts' role seems to be more valued in that their involvement should occur at the design stage of the FRIA, whereas in the former case, the legal text suggests calling them for intervention at a later stage (risk mitigation), that is, after the risk identification process. Similarly, Recital 90 of the DSA advises providers of VLOPs and VLOSEs to involve independent experts in conducting risk assessments and designing risk mitigation measures.

3.4. Stakeholders' Involvement

Stakeholders' involvement constitutes another fundamental aspect that faces significant limitations within current impact assessment models in EU digital policy[64]. The restriction on stakeholder participation raises a notable concern, that is, countervailing interests may not receive due consideration during the crucial phases of risk assessments and the formulation of mitigation measures. In the dynamic and rapidly

[62] A. Mantelero, *Beyond Data,* cit., 19-20.

[63] European Commission, *Cost of the Cumulative Effects of Compliance with EU Law for SMEs*, 2015, 122; B. Mueller, *How Much Will the Artificial Intelligence Act Cost Europe?*, 2021, Center for Data Innovation Report.

[64] A. Christofi et al., *Data Protection, Control and Participation Beyond Consent-Seeking the Views of Data Subjects in Data Protection Impact Assessments*, in E. Kosta-R. Leenes-I. Kamara (eds.) *Research handbook on EU data protection law*, Cheltenham-Northampton, 2022.

evolving landscape of digital technologies, engaging a diverse range of stakeholders is imperative. This inclusiveness ensures the incorporation of a comprehensive array of perspectives, expertise, and potential impacts related to emerging technologies, including, but not limited to, AI.

Without robust stakeholder engagement, assessments may fail to capture the full spectrum of concerns and interests at stake. A more inclusive approach to stakeholder engagement can enrich the assessment process, leading to more nuanced and well-informed evaluations of the risks and benefits associated with technological development. Therefore, addressing the limitation in stakeholder involvement is crucial for fostering a comprehensive and socially responsible approach to governing digital technologies.

In this regard, the GDPR envisages the involvement of data subjects or their representatives in the intended processing, but only where the data controller deems it "appropriate" (Art. 35(9)). Conversely, the AI Act foresees stakeholders' participation in neither the FRIA nor the risk management system requirement. Thus, stakeholders' involvement is only suggested, where appropriate, in relevant recitals[65]. However, it is worth stressing that the original FRIA obligation proposed by the EU Parliament differed. In particular, it required deployers (but for SMEs, which could have voluntarily opted to comply with this provision) to notify relevant stakeholders and, to the best extent possible, involve representatives of the persons or groups of persons that would have likely been affected by the high-risk AI system (such as equality bodies, consumer protection agencies, social partners and data protection agencies) in order to receive inputs into the impact assessment. Those bodies would have had a period of six weeks to respond. Unfortunately, during the trilogue negotiations, this provision was "downgraded" to a recommendation in recitals, which are not binding. Similarly, the DSA contemplates the involvement of relevant stakeholders[66] (e.g., representatives of the service recipients, representatives of groups potentially impacted by their services and civil society organisations) only in recitals[67]. Unlike the other two legal acts, the DSA goes further in suggesting some procedural aspects of this involvement: providers «should seek to embed such consultations into their methodologies for assessing the risks and designing mitigation measures, including, as appropriate, surveys, focus groups, round tables, and other consultation and design methods»[68].

3.5. Controls

Another critical shortcoming of impact assessments for governing the development and use of emerging digital technologies lies in their frequent internal conduction,

[65] Recitals 65 and 96, AI Act.

[66] See R. Griffin, *Public and Private Power in Social Media Governance: Multistakeholderism, the Rule of Law and Democratic Accountability,* in *Transnational Legal Theory*, 14, 2023, 50.

[67] Recital 90, DSA.

[68] *Ibid.*

giving rise to significant concerns regarding potential conflicts of interest[69]. When these assessments are conducted internally by the organisations developing digital technologies, there is a natural inclination for these entities to prioritise their own interests, potentially overlooking or downplaying broader societal implications. This internal approach may inadvertently lead to biased assessments that favour organisational goals over the normative considerations (that is, ethical, social, and legal) that should guide the development of digital systems.

To mitigate this inherent hurdle, there is a compelling need for the implementation of internal and external control mechanisms by independent parties. These mechanisms would serve as a safeguard, ensuring that impact assessments remain objective, transparent, and accountable.

In this regard, the GDPR requires data controllers to designate a DPO in cases of high-risk data processing. The DPO is tasked with informing and advising the data controller on data protection matters and monitoring compliance with the Regulation. In particular, the data controllers must seek their advice when a DPIA must be carried out. The latter point must be highlighted. Thus, the DPO is not tasked to carry out the DPIA but, where requested by the data controller, to provide advice (which is not binding) *and* monitor the performance of the assessment.[70] However, recent data from a report drafted by the EDPB confirm that DPOs are usually tasked with drafting and carrying out DPIAs[71]. At the other end of the spectrum, quite paradoxically, many respondents to the EDPB investigation stated that DPOs are not closely involved in the process of DPIAs[72]. Eventually, even if DPOs can be engaged in drafting a DPIA, they still should retain a sufficient degree of independence[73] to evaluate the impact assessment and its results.

The DSA follows the example of the GDPR and requires VLOPs and VLOSEs to establish an independent "compliance function" led by the compliance officer. The function must monitor the provider's compliance with the DSA[74], including ensuring that the SRA referred to in Art. 34 is carried out and properly reported and that risk-mitigation measures are taken pursuant to Art. 35. In terms of external controls, the DSA requires providers of VLOPs and VLOSEs to undergo independent audits at least once a year to assess compliance with the obligations they are subject to, including the obligation to carry out an SRA. To qualify for such external audits, organisations must meet several criteria in terms of independence, as well as proven expertise, objectivity and professional ethics. Providers shall cooperate and assist auditors in enabling them to conduct such investigations in an effective, efficient, and timely manner.

In the context of the AI Act, whereas forms of external testing/audits are foreseen

[69] F. Ferretti, *Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?,* in *Common Market Law Review*, 51(3), 2014.

[70] Art. 39(1)(c), GDPR.

[71] EDPB, *2023 Coordinated Enforcement Action: Designation and Position of Data Protection Officers,* 2024, 20.

[72] *Ibid.*, 19.

[73] Art. 38(3), GDPR.

[74] Art. 41, DSA.

throughout the Regulation for high-risk AI systems (e.g., third-party conformity assessment procedures; external adversarial testing for general-purpose AI models with systemic risks; etc.), Art. 27 does not include any internal or external controls when a deployer must carry out a FRIA. The application of the Regulation will tell the extent to which the FRIA will be integrated in the DPIA process and will require the involvement of the DPO.

3.6. Publication

A final aspect to be assessed is the extent of transparency of these risk management tools. Publishing the outcomes of such impact assessment models can benefit all the parties concerned. Developers and providers of digital technologies might receive valid inputs to improve the design and functionality of their applications. Also, the decision to publish the impact assessment can be positively seen as a means of demonstrating accountability. Related to that, other relevant stakeholders (users and consumers of such technologies, data subjects, etc.) would be able to gain a better understanding of the risk implications of digital technologies on, say, their fundamental rights and to hold developers and providers accountable for the risk introduced in the society. Moreover, transparent impact assessments might foster an informed public debate on the different normative (ethical, legal and social) implications of emerging digital technologies. As a result, this might strengthen public trust in the "digital revolution", which is an overarching goal of Union's digital policy[75].

Data controllers are not required to publish DPIAs under Art. 35 GDPR. Yet, «controllers should consider publishing them either in full or, at the very least, in summary form. This aligns with the overarching principles of transparency and accountability».[76] Similarly, deployers of high-risk AI systems falling in the scope of Art. 27 AI Act do not have a statutory obligation to publish the outcome of the FRIA. However, it must be highlighted that the Parliament's original proposal for a FRIA contained an obligation to publish a summary of the results of the impact assessment as part of the registration of use for specific deployers (public authorities, Union institutions, bodies, offices or agencies and gatekeepers under the Digital Markets Act)[77]. In contrast, VLOPs and VLOSEs have to make publicly available a report setting out the results of the risk assessment pursuant to Art. 34 DSA as well as specific mitigation measures put in place pursuant to Art. 35(1) DSA as part of their transparency reporting obligations[78].

[75] The objective of enhancing public trust in digital technologies permeates nearly every area of EU digital policy: cybersecurity (Cybersecurity Act, Recital 2); data economy (Data Governance Act, Recital 3); artificial intelligence (Artificial Intelligence Act, Recital 1); online services (Digital Services Act, Recital 3); etc.

[76] E. Kosta, *Article 35 Data protection impact assessment*, cit., 675.

[77] Art. 29a(5), EU Parliament AI Act draft.

[78] Art. 42(4), DSA.

4. Conclusion

This paper provided an analysis of the role and nature of impact assessments in the broader discourse around "digital regulation" in the EU. After having explored the double-faceted nature of impact assessments as part of the policy-making process and as an object of regulatory action, we focused on the second aspect. In this regard, we analysed three impact assessment models that are relevant in the EU digital governance: a) the DPIA under the GDPR; b) the FRIA in the AI Act; c) the systemic risk assessment contained in the DSA. Lastly, we critically addressed six normative issues of impact assessment as a regulatory tool (measuring impacts; effective operationalisation; interdisciplinarity; controls; stakeholders' involvement; publication) with a view to steering future digital technologies regulation and compliance in the EU.

The governance trend of increasingly relying on impact assessments has to be read in conjunction with the risk-based and co-regulatory approach of EU digital policy. The integration of impact assessments into the digital regulatory framework reflects a commitment to constraining digital behaviours in proportion to the identified risks. By enforcing specific impact assessments, the EU aims to strike a balance between fostering innovation in the digital sphere and safeguarding fundamental rights, social values, and ethical principles.

Moreover, the regulatory option of heavily relying on impact assessments carried out by private (and public) actors and monitored by specialised state authorities is yet another policy attempt to oversee relevant digital actors and steer digitalisation in a way that it aligns with EU values and principles. On a different level, these regulatory tools, which are increasingly finding consensus among EU policy-makers, might also be leveraged for purposes other than complying with a legal act. In particular, where the addressee of such an obligation is extra-EU, as in the case of the majority of big tech companies, the room for interpretation left by the norms gives national authorities or the Commission (e.g., with regard to DSA's enforcement on VLOPs and VLOSEs or having regard to the enforcement of the AI Act rules on General Purpose AI models and systems) enough flexibility to pursue digital sovereignty aims which that would otherwise fall outside the scope of the evaluation.

Against the background of the extent to which impact assessments in EU digital policy *impact* our society, we deem it essential to ensure a greater degree of transparency and accountability at every level of these regulatory tools, that is, not only at the implementation level but also at the enforcement level. This latter point admittedly relates to another challenge, which nevertheless falls outside the remit of this paper, that is, who controls the controllers[79].

[79] The well-known Latin formula from the Roman satiric poet Juvenal "*quis custodiet ipsos custodes*?" long has animated the debate on (digital) governance. See, for example, L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU,* in *Philosophy & Technology*, 33, 2020, 375.