Vulnerability in the EU AI Act: building an interpretation

Rebrean, M.L.; Malgieri, G.

Vulnerability in the EU AI Act: building an interpretation

Maria-Lucia Rebrean*
Leiden University
eLaw Center for Law and Digital Technologies
Leiden, Netherlands
m.l.rebrean@law.leidenuniv.nl

Gianclaudio Malgieri
Leiden University
eLaw Center for Law and Digital Technologies
Leiden, Netherlands
g.malgieri@law.leidenuniv.nl

Abstract

The EU Artificial Intelligence Act (AIA) integrates the concept of (human) vulnerability as a critical element for categorising high-risk AI systems, prohibiting exploitative practices, and enforcing safeguards for fundamental rights. Yet the Act lacks a unified definition, leading to fragmented and inconsistent application. This paper addresses this gap by proposing a comprehensive framework for understanding vulnerability in the AIA, rooted in interdisciplinary scholarship and EU legal traditions. We argue that vulnerability should be understood as a heightened risk to fundamental rights arising from power imbalances, dependencies, and varying levels of personal or structural resilience. Through a systematic analysis of the AIA's vulnerability-related provisions, we demonstrate how this framework can harmonise its diverse references, inform risk assessments, and guide regulatory enforcement.

CCS Concepts

• **Artificial Intelligence**; • **Law and Policy**; • **Power Imbalances**;

Keywords

Artificial Intelligence Act, Vulnerability, Power Imbalances, Interpretation

ACM Reference Format:
Maria-Lucia Rebrean and Gianclaudio Malgieri. 2025. Vulnerability in the EU AI Act: building an interpretation. In *The 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT '25), June 23–26, 2025, Athens, Greece*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3715275.3732133

1 INTRODUCTION

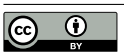
Vulnerability is an intrinsic characteristic of human beings that has been amplified by digitalisation. Digitalisation exposes our lives to addictive social media architectures, manipulative commercial practices, exploitative data collection, more sophisticated forms of discrimination, and much more. The concept of 'vulnerability' has subsequently been adopted into European Union (EU) law, particularly in the realm of digital law. The notion of "vulnerable consumers" was introduced in the 2005 Unfair Commercial Practices Directive (UCPD) [1]. The General Data Protection Regulation (GDPR) [2] is the first 'digital law' that recognises the enhanced vulnerability of online users. Most recently, the Artificial Intelligence Act (AIA) [3] contains numerous references and formulations pertaining to 'vulnerability', the meaning of which was recently considered under the European Commission's (Commission) interpretational guidelines on prohibited AI practices (the Guidelines) [78]. Although the Guidelines advocate that the concept "should be based on a broad spectrum of categories", they refer to purely individualistic elements ("cognitive, emotional, physical and other forms" [78]) of susceptibility, which should be the result of the person belonging to a specific 'vulnerable' group. This paper demonstrates how the Commission's definition might prove incomplete for the inference of the general concept of 'vulnerability' in the AIA. We begin by exploring the theoretical notion of vulnerability from an array of legal and social interpretations (Section 2). We then describe the AIA's references to (human) 'vulnerability' and place them in the presented literature (Section 3). Based on the analysis, we observe a lack of clarity over the meaning of 'vulnerability'[see also: 76, 77] and, therefore, propose a definition of vulnerability that is suitable across the term's uses in the AIA (Section 4). We define human vulnerability as **the higher risk to fundamental rights resulting from power-imbalanced dependencies (at the interplay between personal characteristics, relational situations and socio-techno-economic-political contexts), and personal and structural levels of resilience**.

2 VULNERABILITY

Vulnerability is a concept that infiltrated both academic discourse [e.g., 4, 9, 22, 23, 29, 31] and policymaking [e.g., 5, 6, 7]. The term's omnipresence can be attributed to its capacity to concurrently describe, measure, and analyse a shared yet individualised human experience and the (institutionalised) responses thereto. A generalized definition might frame vulnerability as "susceptibility to harm" [4, 8–10], but its complex, interdisciplinary genealogy points to a richer understanding. Delor and Hubert highlight the term's complexity, suggesting that it encompasses a wide range of concepts, including dependency, fragility, lack of effective regulation, and limited resilience [12]. 'Vulnerability' often functions as a moral and political imperative, and as a mechanism of accountability that prompts relevant societal structures to understand and provide protections adapted to experiences of vulnerability [13, 14].

Despite its definitional complexity, 'vulnerability' has permeated the EU sectoral policy [e.g., 7, 15, 16, 17], expanding into the frameworks regulating the digital domain. 'Vulnerability' was first employed in consumer protection law, serving to distinguish some consumers who were at higher risk of harm when compared to 'average' consumers [5, 10, 18]. However, this distinction has been criticized in the context of digital technologies, where personalization and addictive design can render any individual vulnerable [18].

*The authors have contributed in equal measure.



FAccT '25, Athens, Greece

ACM ISBN 979-8-4007-1482-5/2025/06
https://doi.org/10.1145/3715275.3732133

In the digital sector, the GDPR first introduced the term 'vulnerable data subject', the meaning of which was explained by one of the co-authors elsewhere [19]. Recently, the Digital Services Act makes five references to vulnerability [20, Recitals 62, 69, 94, 95, 104], while the AIA mentions the term 17 times (Table 1). The recitals of these EU regulations offer some examples of (often protected) characteristics attributed to individuals experiencing vulnerability (e.g., age, disability, ethnicity, etc.) but lack a clear definition for the term [see also 21, 100].

Clarifying the meaning of 'vulnerability' is necessary due to its semantic overflow, its prominence in the legal framework and its associated legal roles. Within the AIA such roles include, for example, the term's significance as a criterion for prohibited AI (Art. 5(1)(b)), for expanding the Annex III list of high-risk AI (Art. 7(2)(h)) and for enforcement procedures (Art. 79(2)). Vulnerability should also be accounted for in Fundamental Rights Impact Assessments (FRIA) (Art. 9(9)) and the drafted codes of conduct (Art. 90). Within regulatory sandboxes, personal data can be processed beyond the original purpose to train and test AI systems for the public interest only if (among other conditions) data subjects in a condition of vulnerability due to their age or disability are appropriately protected (Art. 60).

Against this backdrop, **this paper aims to construct an adequate definition of 'vulnerability' and its variations as they appear in the EU AIA.**Inspired by interdisciplinary literature, we observe vulnerability as a dynamic concept [5]. We propose that human vulnerability should be defined as **the higher risk to fundamental rights resulting from power-imbalanced dependencies (at the intersection of personal characteristics, relational contexts, and socio-techno-economic-political situations) and personal and structural levels of resilience**. We observe three interrelated dimensions of vulnerability: power-imbalanced dependencies, resilience, and the interference with fundamental rights.

The necessity of context-sensitive and fundamental-rights-oriented interpretations of vulnerability is also supported by judicial reasoning, particularly within the case law of the European Court of Human Rights (ECtHR). In their landmark analysis, Peroni and Timmer [81] observed that the ECtHR employs a dual conceptualisation of vulnerability: first, as a group-based presumption that calls for special protection, and second, as an individualised condition arising from specific circumstances or contexts. This jurisprudential duality mirrors the theoretical tension between identity-based and universalist approaches, and reinforces the notion that vulnerability can act as a normative trigger for heightened state duties and positive obligations under the European Convention on Human Rights [85]. More recently, Boutier [82] has illustrated how the ECtHR has increasingly used vulnerability not only as a descriptive term but as a legal category that justifies differentiation in the level of protection afforded to certain individuals or groups, especially in migration, detention, and social welfare contexts. This supports the view that legal interpretations of vulnerability are not fixed, but evolve in relation to changing societal risks and power structures, particularly in technologically mediated environments. Complementing this trajectory, Teo [83] has argued that the ECtHR's engagement with human dignity, often entwined with vulnerability, demonstrates that courts are moving toward a more substantive interpretation of dignity as autonomy, equality, and participation. In her view, the interpretive turn toward dignity has reinforced vulnerability's legal salience, transforming it from a passive descriptor into a condition that activates stronger procedural safeguards and interpretive leniency in fundamental rights adjudication [84]. This interpretive lens further justifies treating vulnerability not as a fixed identity but as a legal marker of asymmetrical dependency and the need for responsive institutional design.

In light of these doctrinal developments, the AIA's references to 'vulnerability' should be read not only through the lens of regulatory coherence but also in light of the evolving constitutional practice of human rights courts. This reinforces the paper's proposal to adopt a dynamic, relational, and dignity-sensitive understanding of vulnerability that can operationalise fundamental rights protections in AI regulation.

To validate this approach, we first uncover academic theories of vulnerability (Section 2.1). Then, we outline how the term has been integrated into the AIA (Section 2.2). In the following sections, we examine some of the more frequently used formulations of vulnerability in the AIA (Section 3) and substantiate the proposed definition of the term against the theoretical background (Section 4).

2.1 Exploring vulnerability: an interdisciplinary approach

This section explores the existing theoretical background that can inform the interpretation of vulnerability within the AIA. The term 'vulnerability' raises great disciplinary diversity, being simultaneously employed to describe individual and group relations towards institutions, an emotion, a shared and circular form of social responsibility, a (dis)ability, and a form of legal categorization. As Cole suggests, vulnerability entails "ambivalent potentiality" [4], signifying that it allows for contradictory interpretations and applications. Some of the most prominent theories exploring vulnerability can, broadly, be categorized into the universal-particular (post-identity/identity) dichotomy and the layered perspectives.

Four premises can be summarised to govern the writings of the universalist thinkers [e.g.,13, 25, 27, 29, 30, 31]. The first is that vulnerability transcends identity and is inherent to all human beings due to the human embodiment [29, 30]. The second is that embodiment entails dependence on 'others', including, institutions, family groups [24, 30, 31]. Dependency can be differently experienced based on individual resilience, needs and capability [30, 68], and denotes that human beings are bound to societal structures, acting and integrating within interconnected social environments (however, these may manifest themselves). The third element recognizes that while vulnerability is inherent, the lived experiences thereof are mediated by numerous macro-structural and micro-individual factors, e.g., political system, group belonging, digitalization, etc. Fourth, vulnerability is a criterion for action, care and (moral, political, legislative, interpersonal) accountability [14].

The universalist or post-identity view of vulnerability is contested by perspectives that see it as tied to specific personal elements. The 'particular' or 'identity-based' notions of vulnerability stem from identity politics [4, 22, 35], and link vulnerability to semi-immutable and temporal characteristics that individuals possess or share with others, and which cannot be entirely eradicated [37].

Groups traditionally afforded protection under this framework include children, individuals with disabilities, and those defined by gender-based identities. For policymaking, development and interpretation, this categorical approach to vulnerability has been favoured because it offers greater legal certainty [e.g., 6, 101]. Such identity-based protection is, as Fineman explains, within the ethos of human rights protections [27], but has been criticized for its stigmatization, paternalization and labelling effect [39, 44]. Moreover, in the context of AI system development and deployment, traditional group divisions and identity-based approaches no longer align with the technology's operational character. Machine learning systems, in particular, are characterized by their black-box nature, reliance on fallacious proxies, and tendency to create unknown or unpredictable groupings based on ambiguous data [41, 42]. Given the limitations of universal and particular approaches, it is essential to explore whether transversal interpretations offer a solution for understanding vulnerability in the context of AI development and deployment.

Transversal or 'layered' approaches examine how various spheres of influence, ranging from micro-personal factors to macro-structural elements, interact to shape an individual's or group's perception and experience of vulnerability. For example, Gressel, et. al., present a multi-dimensional model for understanding vulnerability, in which resilience factors, constraints, impacts, and interventions are among the key conceptual elements [43]. Further, Luna posits that vulnerability is comprised of multiple layers, shaped by factors such as time, space, and states, and should therefore be analysed by tracing its origins and its associated cascading effects (or impacts) [39 ,44]. For Luna, each vulnerability layer requires a coordinated response and mitigation strategy [50]. One of the coauthors argued Luna's approach is the most compatible with the digital technologies landscape and the GDPR's risk assessment and mitigation frameworks [19].

One factor left unexplored in the previous dissection is context. This is not to imply that the authors of the different schools disregard context. Instead, it is more intriguing to note how scholars apply the fundamental theories of vulnerability to develop contextually-attuned interpretations of the term. For instance, consumer vulnerability is an application of the 'particular' theories of vulnerability to EU consumer protection law due to the term's explanatory reference to characteristics, such as credulity, age or physical infirmity [e.g., 1, Art. 5; 5, 10, 18, 52, 53]. In turn, 'administrative vulnerability' derives from universal approaches to describe vulnerability as experienced by citizens in relation to (digitally mediated) administrative processes [e.g., 48, 49, 50, 80]. Lastly, data subject vulnerability draws on Luna's transversal theory to address scenarios where individuals may experience vulnerability due to data processing activities and/or their outcomes [7, 19]. These contextual applications reveal the need to use the fundamental interpretations of vulnerability to interpret the term within the AIA. Consequently, it is necessary to observe how the Act references 'vulnerability'.

2.2 Vulnerability: references in the AIA

Complementing the Charter of Fundamental Rights [57] and other sectoral regulations [e.g., 1, 2, 58], the AIA is the newest legal instrument governing AI systems in the EU. The AIA adopts a risk-based model that allocates specific obligations and requirements to AI providers and deployers based on the AI system's risk profile (prohibited AI, high-risk AI, no/limited risk AI, general-purpose AI, general-purpose AI with systemic risks) [32–34]. Excluding those regarding cybersecurity, the AIA makes 17 derivative references to the original term (Table 1) across 9 recitals and 6 articles. Despite these references, and as recognized by the Commission's Guidelines [78], Article 3 of the AIA does not define the term [see also: 76, 77].

The purpose of this article is to supply a definition of 'vulnerability' that is applicable across the Act's references thereto. Clustered, there are 6 formulations presented in the AIA pertaining to vulnerability (Table 1). Each of the formulations is further associated with a series of examples (Tables 2 and 3). The examples do not always impose limitations. Instead, they offer illustrative clarifications and serve to define the context of specific mentions of vulnerability. We organised the examples into five categories: (i) demographic characteristics, (ii) groups, (iii) personal sources of vulnerability, (iv) contexts and (v) no example (Table 2). The first category, **demographic characteristics**, includes specific attributes which influence individual life experience. The second category, **groups**, pertains to historic, protected and collective attributes. The third category, **personal sources**, encompasses volatile traits that are personal but temporal and based on societal, spatial, institutional, political and economic variables. The fourth category, **contexts**, consists of instances that either inherently produce vulnerability or are predisposed to it. The **no example** category is designated for instances where no particular illustration is provided, i.e., wherein the AIA states that market surveillance authorities in EU Member States should account for the impact of AI systems on vulnerable groups (Art. 79(2)).

The **demographic characteristics** are the most employed examples. Across the cumulative 13 mentions, demographic characteristics include age, disability, and gender. Among these, age and disability are the most frequently invoked references, appearing respectively 7 and 5 times. Unlike the specification in the Commission's Guidelines [78], we argue that the 'age' can be interpreted to include all life stages and associated (mental and physical) capacities, denoting that vulnerability may differently occur to everyone throughout one's life. In turn, the notion of disability is quite specific, as Recital 29 of the AIA clarifies that it should be within the meaning of Directive (EU) 2019/882, i.e. "persons who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others" [55, Art. 3(1)]. The references to 'long-term impairments' and the 'barrier-mediated limitations to equal participation in society' appear restrictive, seemingly excluding addictions or temporary conditions. Finally, 'gender (equality)' is only employed once in relation to the horizontal development and application of voluntary codes of conduct (Article 95(2)(e)). Though the term gender is evoked in other instances throughout the AIA [3, Recitals 27, 48, 58, 165 and Article 68], the regulation makes no reference to the understanding of the term despite its fluidity and significance for identity formation [e.g., 56, 57]. With the exception of age, the examples placed under this first category could invoke the 'particular' interpretation of vulnerability (Section 2.1).

Table 1: AIA References and Formulations of 'Vulnerability' – Overview

Reference formulation	Total references	Recital	Article
vulnerabilities of a person/ group of persons	4	29	5.1.b
Children's vulnerabilities	2	48	9.9
[social or economic situation makes] persons more vulnerable to exploitation	1	29	
[natural person in a] vulnerable position	3	58, 60	7.2.h
Vulnerable groups		67	9.9
	7	93	60.4.g
		132	79.2
		141	
[groups of] Vulnerable persons	2	165	95.2.e
	17		

Being an illustration of the regulatory shift from individual- to collective oriented protections [see e.g., 64], the category '**groups'** (Table 2) makes 7 references to racial/ethnic minorities/groups (2), children (2), religious minorities (1), and 'other/certain' groups (2). The first mention of ethnic and religious groups is offered as an example of social situations that might make an individual more vulnerable to exploitation (Table 3) [3, Recital 29]. This reference suggests that an individual's group belonging may amplify vulnerability, increase the likelihood of exploitation, and be an integral to the person's social (or economic) situation. Additionally, Recital 67 of the AIA underscores that AI systems can intensify existing forms of discrimination against "certain vulnerable groups". Racial and ethnic groups are cited as examples of certain groups that have **also faced historical discrimination** [e.g.,: 58, 59, 60]. The example's wording suggests that not all vulnerable groups must have experienced historical discrimination and that other groups may also be considered vulnerable. Among other examples within the groups category, children represent a particularly vulnerable group, not because of historical discrimination. According to Kurian, children are vulnerable due to, for example, their developing capacities and limited (emotional) resilience [61]. Mentioned narrowly also as "persons under the age of 18" [3, Art. 9(9)], children are afforded additional protection under EU (digital) law [e.g., 62, 63]. In the AIA, the particular vulnerabilities of children must be given special consideration within the AI provider's risk management system [3, Art. 9(9)], which includes the completion of a FRIA [3, Art. 9(1)]. Notably, the risk management system should not only reflect on children, but also on "other" vulnerable groups [3, Art. 9(9)]. This phrasing may permit a broader interpretation of vulnerable groups, encompassing, at minimum, racial and ethnic groups, and extending to considerations of socioeconomic conditions.

The **personal sources** of vulnerability (9) were predominantly used within provisions outlining the expansion of the list of high-risk AI systems (Articles 7, 7(2)(h), 7(2)(g), Annex III) and in relation to migration or public administration processes (Recital 58). These contexts are closely associated with the concept of 'vulnerable position' (Table 1, Table 3). As a result, vulnerability could be understood as both a condition shaped by external circumstances and as an attribute connected to the individual's inherent characteristics (See also Section 2.1.). The connection between the 'vulnerable position' and the high-risk contexts seems evident, as these situations often create the highest risk to rights and the most significant experiences of dependency and power imbalances. Including examples such as health, poverty, and maternity (Table 2), the third established category demonstrates that experiences of vulnerability can also be volatile in relation to both a personal situation and the context in which that situation occurs. Whereas situations of extreme poverty are provided as an example towards the meaning of socio-economic circumstances [3, Recital 29], the evoked elements of status, authority and knowledge are later used as examples of situations of power-imbalance (Table 2) [3, Article 7(2)(h)]. This might suggest that the presence of socio-temporary characteristics can contribute to an individual's vulnerability, with each characteristic (authority, status and knowledge) representing a potential moment of power-imbalance, particularly in relation to several forms of deployers, and deployment contexts. As Recital 93 recognizes, deployers are in unique positions to understand the manifestation of vulnerability, precisely because they have some capacity to redress or participate in the relevant decision-making. The socio-temporal characteristics category also includes the notion of dependent/dependency making it possible to conceive of the concept as an essential element to understanding vulnerability [see also: 24, 27, 31].

The combination of the example categories (Table 2) and the theoretical framework (Section 2.1) underscores the importance of an adaptive, multi-dimensional interpretation of vulnerability in the AIA that accounts for risks to rights, contextual factors, and power imbalances. However, it is essential to consider that, given the limitations of particular provisions, significant forms of vulnerability may still be overlooked. For example, Article 5(1)(b) does not mention vulnerability situations in relation to victims of gender-based violence, non-disabled patients, gamblers, and individuals addicted to social media unless we adopt a broader interpretation of 'specific social situation' or 'disability.' Additionally, the references to 'specific social situation' do not necessarily but could encompass the experiences of employees or healthy patients, recognising that these groups may still face power imbalances and exploitation risks. These points call for a more inclusive interpretation of vulnerability. Noting these possible exclusions and the importance of an adaptive understanding of vulnerability, the following sections explore the meanings of 'vulnerable position', 'vulnerable groups', and the meaning of vulnerability in the AIA prohibitions in more detail.

Table 2: Examples provided regarding 'vulnerability' in the AIA

Total Mentions		**Recitals**	**Articles**
Mentioning of Demographic factors of vulnerability	**13**		
Age		29	5.1.b.
	7	58	7.2.g.
		132	9.9
			60.4.g
Disability		29	5.1.b.
	5	132	60.4.g
			95.2.e
Gender [equality]	1		95.2.e
Mentioning of specific Groups of vulnerability	**7**		
Racial/Ethnic Minorities/"Groups"	2	29, 67	
Children/persons under the age of 18	2	48	9.9
Religious Minorities	1	29	
Other/Certain Vulnerable Groups	2	141	9.9
Mentioning of "personal sources" of vulnerability	**9***		
Extreme Poverty	1	29	
Status	1		7.2.h
Knowledge	1		7.2.h
Authority	1		7.2.h
Dependency/ dependent on outcomes	1	58, 60	7.2.g*
Maternity	1	58	
Health [illness]	1	58	
Unemployment	1	58	
Housing assistance	1	58	
Mentioning of "contexts" of vulnerability	**8**		
Social/economic conditions or situation [including extreme poverty, ethnic or religious minorities]	3	29	5.1.b
			7.2.h.
Public administration services [provided in cases of socio-temporal characteristics]	1	58	
Migration [asylum, border control management]	1	60	
Persons who are potentially harmed/ suffer adverse impacts/ likely to be affected	2	93	7.2.h
Power imbalances [status, authority, knowledge]	1		7.2.h.
No example	**2**	165	79.2

**Note: Article 7(2)(g) of the AIA references 'dependency,' not 'vulnerability.' Thus, while excluded from the vulnerability count, its relevance to high-risk AI designation warrants its inclusion in the table.*

3 EXPLAINING NOTIONS OF VULNERABILITY IN THE AIA

The preceding sections reviewed key theoretical frameworks informing the interpretation of 'vulnerability' (Section 2.1) and provided a descriptive analysis of the term's references within the AIA (Section 2.2). The associated formulations and examples within the AIA underscore the need to understand vulnerability as a multi-dimensional concept. The following sections examine the implications of three specific formulations: (i) vulnerable position, (ii) vulnerable groups, and (iii) vulnerability within the purview of the prohibition in Article 5(1)(b) of the AIA (Section 3). We selected these formulations based on their relevance and illustration of the discussed vulnerability frameworks (Section 2.1). 'Vulnerable position' reflects universal approaches to vulnerability, while 'vulnerable groups' aligns with 'particular' perspectives. Lastly, we analyse 'vulnerability' with the AIA prohibition in relation to the Commission's Guidelines draft definition of 'vulnerability' [78]. Building on this analysis, we then substantiate our proposed definition of vulnerability (Section 4).

3.1 Vulnerable Position

The 'vulnerable position' formulation is present in Recitals 58 and 60 and Article 7(2)(h) of the AIA (Table 1). Recital 58 outlines why certain types of AI systems used in public administration are deemed to be high-risk under the AIA. It stipulates that individuals depend significantly on the outcomes produced by these systems, which can profoundly impact an individual's well-being and fundamental rights. Individuals are, therefore, in a "vulnerable position in

Table 3: Examples employed in relation to each of the formulations of vulnerability in the AIA

Reference formulation	Total ref.	Examples in reference formulation
vulnerabilities of a person/ group of persons	**4**	Age, Disability Socio-economic situations
Children's vulnerabilities	**2**	Children & persons under the age of 18
[situation makes] persons more vulnerable to exploitation	**1**	Socio-economic situations (incl. extreme poverty, ethnic and religious minorities)
[natural person in a] vulnerable position	**3**	All examples in Socio-temporal characteristics (Table 2); Socio-economic situation Migration and public administration services Persons who are potentially harmed/ suffer adverse impacts
Vulnerable groups	**7**	Age, Disability Racial and ethnic minorities 'other' (Article 9.9), 'certain' (Recital 141)
[groups of] Vulnerable persons	**2**	Disability, Gender (equality)
	17	

relation to the deployer" [3, Recital 58] of the AI system. Applying similar reasoning, Recital 60 recognises that natural persons occupy a vulnerable position in relation to high-risk AI systems deployed in asylum and migration contexts. Given these two recitals, it is unsurprising that within the criteria set out in Article 7 for the expansion of Annex III of the AIA, we find the term 'vulnerable position'.

In particular, Article 7(2)(h) links the individual's vulnerable position to situations of power imbalance. Drawing on Recitals 58 and 60, contexts of significant power imbalance can be interpreted as situations of dependency on deployers, AI-generated outputs, and potential risks to fundamental rights and include, at minimum, public services and migration. Article 7(2)(h) clarifies that power imbalances in relation to deployers may occur "in particular due to status, authority, knowledge, economic or social circumstances, or age". With the exception of the demographic 'age' characteristic (understood to include the entire lifespan, see Section 2.2), these examples are **personal sources** of vulnerability (Table 2). Both age and other socio-temporal characteristics can vary widely among individuals, encompassing diverse experiences and applications. By way of Recital 29, it is also clear that economic and social circumstances include an analysis of factors such as extreme poverty or belonging to ethnic or religious minorities (see Table 2 and Section 2.2). A detailed examination of each example's role in contributing to power imbalances in AI and the conceptualisation of human capabilities in relation to high-risk AI systems falls beyond the current scope. Nevertheless, digital technologies have been discussed in legal scholarship as instruments of power and power maintenance [e.g., 65, 66, 67]. Consequently, we can presume a power imbalance exists between the developers and deployers of high-risk AI systems and affected individuals. Together, the employed examples can be considered alongside universal or transversal interpretations of vulnerability (See Section 2.1).

Universal and transversal interpretations of vulnerability assume that all individuals are inherently vulnerable and specify that vulnerability may still be uniquely experienced by each individual (Section 2.1). While transversal approaches may look towards sources or origins of vulnerability and the associated cascading effects [39, 44] (here, e.g., age, illness), universal approaches highlight that individuals are prone to experience dependency on societal structures [22, 27] (here e.g., public administration, migration structures). Regarding transversal approaches, factors such as age, authority, and status that are employed in the AI in relation to 'vulnerable position' can serve as what Luna described as "origins of vulnerability," while the associated increased risk to fundamental rights and dependency emerge as possible "cascading effects" [39, 44]. A similar conclusion has been reached regarding the interpretation of the GDPR's "vulnerable data subject", indicating that transversal approaches could be applied in interpreting 'vulnerability' within EU digital law [19]. Even earlier, in its 2016 report, the Commission emphasized that 'vulnerability drivers' (e.g., behavioural, accessibility-related and situational) should be analysed in relation to the risk of negative outcomes on a consumer's wellbeing [45]. The report also recognises universal approaches to vulnerability, noting that 'vulnerability' can be understood "as a spectrum rather than a binary state" [45].

The Act's contextual approach to understanding 'vulnerable position' that focuses on power imbalances and dependency relative to AI deployer and deployment in specific situations (e.g., public administration and migration), illustrates that individuals may be inherently vulnerable in particular settings. This interpretation is also visible in the reasoning for high-risk classification, wherein some AI deployment settings are considered high-risk due to the potential negative effects they may produce on fundamental rights and due to the individuals' dependency on the AI output.

The 'vulnerable position' expansion criteria in Article 7 are further linked to the criteria of dependency and resilience, as also highlighted by Recitals 58 and 60. Dependency can be understood through the lens of universal vulnerability interpretation. As early as 1987, theorists accounted for indirect and direct forms of dependency as factors contributing to the vulnerable experience [11]. Fabiani and Theys suggest that direct dependence results from,

among other, limited autonomy, and specialization. Indirect dependence is attributed to factors such as interconnectivity [11]. Similarly, Boublil writes that relations of (inter)dependency are intrinsic to the human condition and societal specialisation, thereby creating a form of (moral) social obligation and responsibility to address others' needs [68]. Dodds also proposes that dependency occurs only in specific contexts where individuals rely on others to meet their needs [30] She argues that dependency can be viewed as a form of vulnerability, allowing vulnerability to exist independently of direct reliance on others [30]. This distinction enables broader structural vulnerabilities to be addressed through systemic or institutional protections [30]. Also a proponent of institutional responsibility, Martha Fineman proposes that "individual dependence on social institutions is constant but the nature of that dependence varies and fluctuates over time in response to the circumstances or developmental stage in which we are located" [69]. At the core of these approaches lies the requirement to understand structural-individual relations that consolidate fluctuating experiences of dependence and vulnerability. For the purposes of this paper, the discussed theoretical background highlights that dependency on an outcome produced by AI systems within contexts prone to power imbalances can render any individual in a 'vulnerable position', and that it is necessary to look at avenues for (institutional) resilience to assess and address dependency.

In regard to resilience and dependency, Article 7(2)(g) specifies that dependency may occur "in particular because, for practical or legal reasons, it is not reasonably possible to opt out from that outcome." Article 7(2)(g), therefore, covertly introduces resilience as another key factor related to dependency and 'vulnerable position'. Fineman views resilience as an incomplete response to vulnerability, characterizing it as both an individual and social attribute [70]. She argues that resilience equips individuals with the means and capacity to recover from harm, setbacks, and life's misfortunes, situating it within a broader network of resources or human capital (e.g., social, ecological, physical assets) [70]. When it comes to understanding the meaning of 'vulnerable position', Fineman's construction of resilience serves the observation of (socially structured/personal) capabilities to withstand unfavourable and potentially unfair AI outcomes. In this context, resilience operates as an ex-post dimension of vulnerability, or, drawing on Fineman's authorship, a mechanism through which individuals can resist and recover from the impacts of AI-driven outputs. When mentioning "practical or legal reasons", the specification in Article 7(2)(g) emphasizes the structural factors that impede an individual's resilience for opting out. For instance, it is hardly imaginable that an individual can opt out of administrative processes precisely because they are structurally (see also legally) mandated. Equally, "practical (. . .) reasons" shows the need for an analysis of the available and differing individual capacities that prevent the person from opting out. Opting out serves as a form of power-balancing strategy. However, while this approach appears promising, digital capabilities and opt-out mechanisms are often ineffectively leveraged within the EU digital legal system, as the private sector employs various techniques to invoke the user's cognitive biases to receive consent. In sum, Article 7 allows for a universal-oriented, political and social lens in interpreting 'vulnerable position', providing clarity on how the EU regulator views critical concepts like power imbalances and dependency. However, this Article remains a political component of the law rather than a directly enforceable provision. In contrast, Recitals 58 and 60 establish some explanatory basis for categorizing certain types of AI as high-risk. The high-risk classification is more binding because it imposes enforceable obligations.

The instances in the AIA that reference 'vulnerable position' share several key features: they (i) omit strictly identity-based characteristics, implying that vulnerability is a universal possibility (ii) emphasize the relational dynamics between AI deployers and individuals, depicting these relationships as susceptible to dependency or power imbalances; (iii) signal that such contexts may pose significant risks to fundamental rights and (iv) support a rationale for the classification of certain AI systems as high-risk. Based on the analysis, a 'vulnerable position' can be understood as a condition in which individuals are exposed to higher risks to fundamental rights due to dependency, limited resilience and power imbalances in relation to AI deployers. This definition aligns with universal understandings of 'vulnerability'. Notably, the term 'vulnerable position' is only one of the AIA's vulnerability formulations (Tables 1 and 3). To move towards a comprehensive definition, the following section analyses the formulation 'vulnerable groups and persons'.

3.2 Vulnerable Groups and Persons

The previous section concluded that the formulation 'vulnerable position' reflects a universal interpretation of vulnerability. In this section, we examine how this interpretation may differ when applied to the terminological derivative 'vulnerable groups' and 'vulnerable persons' (Tables 1 and 3). The term 'vulnerable groups' is the most frequently used of all vulnerability-related terms in the AIA, appearing in seven provisions: Recitals 67, 93, 132, and 141, and Articles 9(9), 60(4)(g), and 79(2) (Table 1). Given their shared interpretation rooted in identity-based approaches to vulnerability (Section 2.2), the aforementioned provisions are analysed alongside those referencing 'vulnerable persons' (Recital (165) and Article 95) and 'children' (Recital 48 and Article 9(9)) (Table 1). It is only Recital (93) that revisits the previously discussed relationship between deployers and affected individuals (Section 3.1), underscoring that deployers are best positioned to understand the impacts of AI systems on vulnerable groups. The remaining provisions highlight the significance of vulnerability across different sections of the legislation, namely: high-risk AI, generative AI (genAI), testing in real-world conditions and market surveillance.

In relation to the risk classification, Recital 48 explains that the assessment of an AI system's adverse impact on fundamental rights is an essential criterion in the high-risk classification. It emphasizes that children's rights should be protected and that "children's vulnerabilities" have been recognized in international legal instruments [e.g., 53, 54, 71]. Though children are often acknowledged as a particularly vulnerable group, 'childhood' is a developmental stage, meaning that there is no one-size-fits-all description of a 'child'. Therefore, literature concerning children's vulnerability online has applied both 'particular' [86] and 'universal' interpretations [72] of vulnerability. In both applications and in the AIA, significant arguments are made to provide children with additional, yet appropriate protection for their online activities. In addition, Article 9(9) mandates that providers consider and mitigate risks

arising for "children and other vulnerable groups" within their risk management frameworks, including FRIAs. It is evident that within the purview of Article 9, the AIA adopts an identity-oriented interpretation of vulnerability by prompting a classification exercise that consequently identifies certain groups as vulnerable and others as 'not vulnerable'. Read in conjunction with Recital 67, it would be unsurprising if this exercise will be based on historical groupings of discrimination. Recital 67 highlights the risk of discrimination that may arise during the development of high-risk AI systems, particularly affecting racial and ethnic minority groups, due to the use of inherently biased datasets [see e.g., 42]. Corresponding to the requirements of Article 10, the recital underscores the need for preventive measures in the datasets utilized by AI providers. The recital's focus on biased (historical) data aligns with an identity-oriented approach to vulnerability (Section 2.1). This interpretation recognizes the need to protect specific (vulnerable) groups whose characteristics have historically been, and continue to be, drivers of societal discrimination and oppression. However, the issue of the adequate protection of overlapping and cumulative traits, remains a significant and unresolved challenge. Recital 132 shifts focus from high-risk AI to the individual-genAI interaction. It emphasizes the risks of impersonation or deception and the need to implement transparency requirements considering the characteristics of persons belonging to vulnerable groups due to age and disability. Depending on deployment and use context, the recital specifies that providers and deployers of genAI systems are not obliged to display transparency notices if it is apparent to a "reasonably well-informed, observant, and circumspect" individual that they are interacting with a genAI system. Given that genAI is often considered an example of general-purpose AI (GPAI) under the AIA [3, Recital 99], similar language appears in Article 50(1), which addresses transparency obligations for GPAI providers, though without the mention of vulnerability. The wording in both provisions can be analysed on the basis of a similar debate surrounding the distinction between 'average' and 'vulnerable' consumer in the UCPD [1, Art 5].

In their analysis of "digital vulnerability" within EU consumer and digital law, Helberger et al. concluded that the average-vulnerable consumer dichotomy is a fallacy, as virtually all consumers may be rendered vulnerable due to power imbalances stemming from malicious design practices, personalization, profiling, and data collection and management [18]. As we also contend and the EU endorsed in its 2016 report [51], Helberger et al. advocate for a dynamic understanding of vulnerability in digital contexts that aligns with universal approaches to vulnerability [18]. This raises the question about how the "reasonably well-informed" individual might be distinguished from the vulnerable individual within human-(gen)AI interactions. In light of these analyses, it is challenging to distinguish between a "reasonably well-informed" natural person and one who is part of a vulnerable group. Recital 132 further specifies that transparency notices should consider the "characteristics of natural persons belonging to vulnerable groups due to their age and disability." As discussed, age can be interpreted universally, while disability may not encompass all short-term disabilities. Unfortunately, this adaptation is limited to cases where the intended purpose of the AI system specifically targets those groups, weakening the requirement. This approach in Recital 132 leads to an identity-based interpretation of vulnerability by linking it to specific characteristics, such as age and disability. Further, the AIA addresses 'vulnerable groups' in relation to real-world testing conditions [3, Recital 141, Article 60(4)(g)] and codes of conduct [3, Recital 165 and Art 95]. Recital 141 specifies that real-world testing of AI systems should incorporate additional safeguards for "certain vulnerable groups". No specific examples are provided on what constitutes a vulnerable group in this case. However, based on the previous analysis, it is clear that they should include religious and ethnic minorities and children. Examining the associated Article 60(4)(g), safeguards should also be directed toward groups defined by age and disability. However, the absence of clarifications on the nature or scope of these safeguards leaves their practical application ambiguous or dependent on collaborative governance mechanisms [e.g., 73, 74]. The identification of specific groups reflects an identity-based interpretation of vulnerability by focusing on specific, predefined characteristics. This interpretation raises questions about how AI systems might address vulnerabilities that extend beyond these fixed categories. Without further concrete examples, this interpretative gap could lead to inconsistent or inadequate protections for other vulnerable groups in the real-world testing procedures. Next, Recital 165 and Article 95(2)(e) of the AIA provide a framework that links voluntary codes of conduct to the protection of vulnerable persons, with a particular emphasis on disability and gender (equality) [3, Recital 165 and Art 95(2)(e)]. Article 95(2)(e) specifically encourages those drafting and implementing these codes to consider the impacts of AI systems on "vulnerable persons or groups of vulnerable persons," highlighting accessibility for individuals with disabilities and the need to uphold gender equality. This explicit mention of disability and gender signals an identity-based interpretation of vulnerability, once more recognizing that certain demographic characteristics (Table 2) significantly influence how vulnerability should be understood in the AIA. In addition, the provision also suggests the types of adverse effects and associated risks that should be examined within the vulnerability analysis.

Lastly, Article 79(2) of the AIA stipulates that market surveillance authorities should pay particular attention to vulnerable groups during investigations. Although no examples are provided, the investigations of vulnerability is key because both providers and deployers must prioritise the protection of vulnerable groups within their risk management systems and deployment activities, as vulnerability often signals heightened risks to fundamental rights. Additionally, evaluating the impact on vulnerable groups can lead to a prohibition of the investigated AI practices (see Section 3.2).

In summary, the AIA's use of 'vulnerable groups' and 'vulnerable persons' reflects a predominantly identity-based approach to understanding 'vulnerability'. These formulations focus on demographic characteristics like age, disability, gender, and historically marginalized identities. 'Vulnerable groups' can be understood under the AIA **as populations that may face heightened risks due to shared attributes,** e.g., children, racial and ethnic minorities, and individuals with disabilities. The same interpretation can be applied to 'vulnerable persons' or 'groups of vulnerable persons'. The reliance on such characteristics can be linked to identity-oriented interpretations of vulnerability and has been previously justified

in legal practice due to legal certainty (See Section 2.2.). Regarding these formulations, the AIA strives to implement safeguards, transparency measures, and impact assessments for these groups, but lacks specific guidelines for applying these protections. This interpretative gap draws inconsistent protections and underscores the need for clearer guidance to effectively support all vulnerable populations. To complete the interpretation of vulnerability under the AIA, which has, thus far, shown to include both universal and identity-oriented perspectives, the next section will examine the Act's prohibition on the exploitation of vulnerabilities.

3.3 Vulnerability in the AI systems prohibitions

The previous sections drew attention to the most employed formulations of 'vulnerability' within the AIA, associating 'vulnerable position' with universal understandings of vulnerability (Section 2.1) and 'vulnerable groups" with identity-oriented interpretations of vulnerability (Section 2.1). The current section is devoted to understanding the implications and flaws of the Commission's provided definition of the notion of vulnerability within the Guidelines [78]. Analysing the Commission's conceptualization of vulnerability permits a suggestion to the improvement of the Commission's proposed definition, and serves the overarching purpose of this paper, which is to develop a definition of vulnerability that addresses all iterations of the term within the AIA. In addition, the choice to focus on this prohibition is justified by the article's relevance to the Act's enforcement.Article 5(1)(b) prohibits the commercialization or use of AI systems exploiting human vulnerabilities and that (aim to) distort behaviours with the effect or risk of causing significant harm. The Commission's Guidelines suggest that vulnerability should be understood as "a broad spectrum of categories, including cognitive, emotional, physical, and other forms of susceptibility that can affect the ability of an individual or a group of persons to make informed decisions or otherwise influence their behaviour" [78]. The institution notes that such vulnerability, within the purview of Article 5(1)(b), is limited to susceptibility resulting from the demographic characteristics of 'age, disability and socio-economic situation' [78]. Later on, the Commission interprets age in reference to numerical extremes (young, old), and, adding to the examples listed in Recital 29 of the AIA (Table 2), socio-economic situation as a "legal status or membership to a specific vulnerable social or economic group", such as belonging to an ethnic minority, religious group, having migrant status or being unemployed [78]. As mentioned in Section 2.2, disability is interpreted with reference to Directive (EU) 2019/882 [55, Article 3(1)], seemingly excluding long-term and temporary impairments. The Commission's proposed definition provides a good starting point for understanding vulnerability, yet lacks a few elements in order for it to be comprehensively applicable to the entirety of the references present within the Act.

Firstly, while we agree that the analysis of individual susceptibility offers a legally certain way of understanding the notion of vulnerability in relation to the development and deployment of AI systems, we want to emphasize that such susceptibility may not only stem from personal characteristics, such as emotions or cognitive and physical capacities, and may require the interpretation of 'socio-economic characteristics' beyond legal status or group belonging. The proposed limitations to both the nature of susceptibility and the understanding of 'socio-economic' characteristics seemingly exclude contextual and relational factors that, along with the previous analysis (Section 2.2, Table 2), equally contribute to situations of experienced vulnerability. It is not only the individual or personal characteristics alone that create experiences of vulnerability. Instead, the form of **power-imbalanced relationship** that characterises AI deployment (e.g., within high-risk scenarios such as public administration or migration), combined with (temporal, cultural and social) **context** that shape not only the development of AI but also the effects of the AI deployment, can produce 'susceptibility'. We, therefore, propose interpreting 'socio-economic characteristics' with a larger scope, and the notion of 'other susceptibilities' as including contextual and relational factors.

Secondly, we believe that limiting the proposed definition to assessing the effects on informed decision-making and behaviour might only be suitable for the interpretation of vulnerability within the prohibition, but not in relation to the other formulations of 'vulnerability' within the AIA. In line with universalist approaches and the 'vulnerable position' formulation of the Act, decisions can be made about you (with or without your knowledge or consent) that render you vulnerable without necessarily changing your behaviour. Instead, such decisions can have an effect on life opportunities or the fulfilment of rights, amounting, in some cases, to rights violations or different types of (non-behavioural) harm. Using Luna's transversal theory of vulnerability [39, 44] (Section 2.2), the changes to one's behaviour and decision-making after such a decision has been passed amount to 'cascade effects' of the experience of vulnerability. Therefore, the experienced personal, contextual and relational 'susceptibility' simultaneously affects behaviour and decision-making as well as life opportunities and the likelihood of harm.

Lastly, the proposed definition does not account for available forms of resilience that can diminish experiences of vulnerability. Such resilience can be viewed as either a reflection of personal or structural forms of available resources that diminish the harmful effects of the experienced vulnerable situation. Under Fineman's scholarship, personal resilience could be viewed as various forms of resources [69]. In turn, structural forms of resilience complement the latter type of resilience and can be understood both in terms of the existence of legal safeguards or institutional mechanisms for both protection and aid. Notably, both Fineman [69] and Teo [83] recognise the dual nature of resilience as consisting of both personal and structural availabilities. The following section will be dedicated to the creation of an adequate definition for understanding the term 'vulnerability' and its associated references within the AIA.

4 OVERARCHING DEFINITION (IT'S NOT WHAT YOU THINK, I CAN EXPLAIN)

The previous analysis concluded that vulnerability within the AIA has been used both as a group characteristic and as a term depicting a power-imbalanced situation. With a view towards the AIA's risk-based approach and aim to protect fundamental rights, as well as the Commission's proposed definition within the Guidelines, we propose that vulnerability should be interpreted as **the higher risk**

to fundamental rights resulting from power-imbalanced dependencies (at the interplay between relational experiences and socio-techno-historical-political contexts) and personal or structural levels of resilience. Notably, we do not necessarily claim that vulnerability is disabling, but rather a state through which it is possible to observe areas where help, protection or empowerment of any kind is needed. In the following, we explain each of the definitional components and encourage courts and interpreters to follow a step-by-step analysis as described.

The first element, namely '**higher risk to rights'**, expands the Commission's understanding of vulnerability [78] (Section 3.3) as susceptibility to behavioural or decisional alteration to provide a more comprehensive scope. Specifically, the notion of higher risk to rights can be adapted to the understanding of the term within the different risk categories, e.g., being unacceptable risk to rights in the case of the prohibitions, or high-risk to fundamental rights in the case of high-risk categorisation. With regard to GPAI systems, the concept of vulnerability may extend to individuals exposed to systemic risks. Further, this proposal aligns not only with the AIA's overarching goal of safeguarding human dignity and autonomy, but in line with the similar dynamic understanding also proposed by Helberger et. al. [4, 18] permits a practical interpretation for courts.

The second element **is power-imbalanced relations** that create **dependencies**. Within the AIA, policymakers have recognised that certain situations place deployers in positions of higher power, rendering individuals in a vulnerable position in relation to the deployer (Section 3.2). Accordingly, research suggests that the mere use and development of AI systems on the basis of flawed or erroneous data [e.g., 41, 42], as well as the presence of decision-making architecture that is prone to manipulation [18, 76] renders the individual in a vulnerable position in relation to both large tech conglomerates and deployers. Notably, the effect and nature of this power imbalance are dictated by both context and resilience.

The third element of **context** implies conducting an assessment of the social, technical, cultural and other structural elements that have led to the use or deployment of the AI system. As highlighted by Boutier [82], such considerations are already part of court rulings in relation to vulnerability. In turn, the fourth element of **resilience** is understood as being composed of two elements. Resilience may be shaped by formal structural factors, e.g., legal frameworks, welfare schemes, or the provision of in-platform settings. This allows individuals to understand, challenge and receive remedies for decisions made by AI systems. Additionally, resilience is also viewed in terms of individual capacities to mitigate or prevent harm, including the ability to understand one's rights and utilize in-platform settings, access financial resources to buffer against harm, or opt for alternative non-platform solutions.

To translate our definition into actionable regulatory guidance, we examine how its core elements interact in practice. The following examples illustrate that vulnerability does not arise solely from individual traits, but rather from the configuration of power relations and institutional frameworks surrounding the deployment of AI. First, consider AI-driven recruitment systems that analyse candidates' behaviour, language, or inferred emotional traits during video interviews. These tools often replicate assumptions about confidence, fluency, or expression, i.e. traits that are culturally or cognitively coded. A queer candidate from a racialised background or with speech disfluencies may be disproportionately disadvantaged. However, the significance of this vulnerability cannot be inferred solely from identity. The core issue lies in the relational dependence between the candidate and the employer. In highly competitive labour markets, particularly those lacking robust anti-discrimination enforcement or unemployment support, the employer holds disproportionate power. The candidate may feel compelled to conform to opaque behavioural norms imposed by the AI system, with no real possibility of contestation or opting out. This relational asymmetry is exacerbated in contexts where structural resilience is weak: where welfare systems are limited, anti-discrimination laws are underenforced, or social stigma deters complaint. Conversely, in jurisdictions with active labour unions, accessible legal redress, and unemployment protections, the same AI deployment may pose a less acute risk, as institutional buffers mitigate individual dependency. Thus, the vulnerability in this scenario emerges from a triangulation of personal features, relational inequality, and structural deficit—a dynamic that the AIA's risk-based logic must be equipped to address.

A second example concerns the use of emotion recognition or behavioural analysis tools in asylum procedures and border management systems, increasingly deployed to detect deception or assess "credibility." Here, the relational asymmetry is stark: the individual is placed in a position of existential dependence on the judgment of the border authority, who holds the discretion to determine legal status, detention, or deportation. In this context, vulnerability does not stem merely from personal distress or trauma, but from the power imbalance that defines the interaction. This dependency is aggravated when structural resilience mechanisms are absent, such as when asylum seekers lack access to interpreters, legal aid, psychological support, or mechanisms to challenge algorithmic assessments. The situation is further intensified in countries with restrictive asylum policies or histories of discriminatory migration enforcement, where trust in institutions is already eroded. Crucially, even a person with high personal coping capacity may remain structurally vulnerable if the legal and social environment offers no avenues for recourse or support. A transversal vulnerability analysis, as proposed in this paper, compels regulators to assess both the system's design and the institutional conditions surrounding it. In such cases, the AI system may not only be high-risk under Annex III, but, depending on how it exploits distress or dependency, could fall within the scope of prohibited practices under Article 5(1)(b).

5 CONCLUSION

The article sought to propose a definition of the term 'vulnerability' and its various iterations within the EU AIA. To do so, we clustered the various references to vulnerability in the AIA and interpreted them in relation to existing theoretical frameworks of vulnerability. Based on the analysis, we propose that vulnerability should be understood as the **higher risk to fundamental rights** resulting from **power-imbalanced dependencies** (at the interplay between relational experiences and socio-techno-historical-political-economic contexts) and personal or structural levels of **resilience**. The paper contains a visual illustration of the proposed definition.

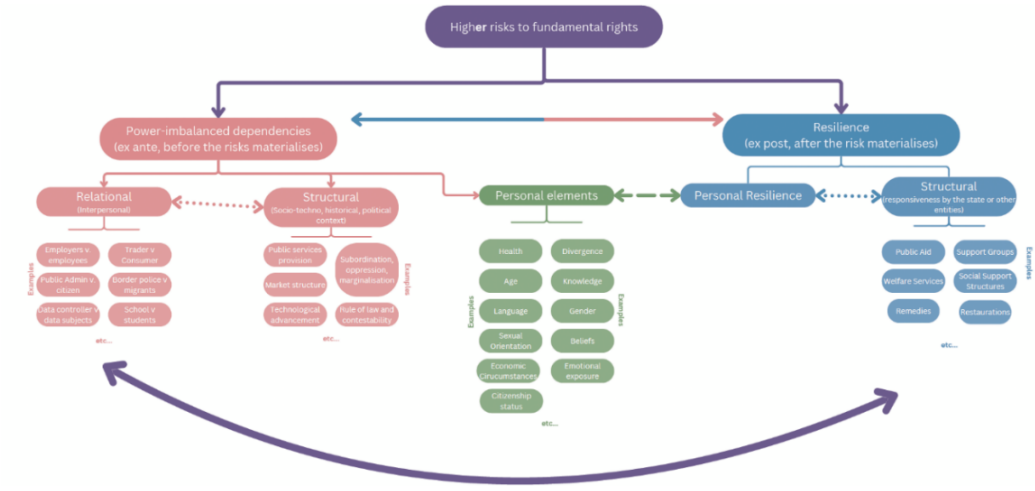


Figure 1: Proposed definition of vulnerability, starting from the AI Act

Acknowledgments

This research was part of RESOCIAL, funded by the Dutch Research Agenda, grant agreement NWA.1540.21.001.

References

[1] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

[4] Alyson Cole. 2016. All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique. Critical Horizons, vol. 17, no. 2, pp. 260–277, doi: 10.1080/14409917.2016.1153896.

[5] Natali Helberger, Kas Betül, Hans-W. Micklitz, Monika Namysłowska, Laurens Naudts, Peter Rott, Marijn Sax, Michael Veale. 2024. Digital Fairness for Consumers. The European Consumer Organisation (BEUC), Brussels.

[6] Nikolina Šajn,. 2021. Vulnerable consumers. European Parliamentary Research Service, PE 690.619.

[7] Gianclaudio Malgieri. 2023. Who is the vulnerable individual?. in Vulnerability and Data Protection Law, 1st ed., Oxford University PressOxford pp. 47–76. doi: 10.1093/oso/9780192870339.003.0003.

[8] W. Neil Adger. 2006. Vulnerability. Global Environmental Change, vol. 16, no. 3, pp. 268–281, doi: 10.1016/j.gloenvcha.2006.02.006.

[9] Roberto Andorno. 2016. Is vulnerability the foundation of human rights? in Human Dignity of the Vulnerable in the Age of Rights, vol. 55, in Ius Gentium Series, vol. 55. pp. 257-272. Dordrecht: Springer.

[10] Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Martin Sax, and Joanna Strycharz. 2021. EU Consumer Protection 2.0 Structural asymmetries in digital consumer markets. The European Consumer Organisation (BEUC), Brussels.

[11] Jean-Louis Fabiani and Jacques Theys. 1987. La société vulnérable : évaluer et maîtriser les risques. Presses de l'École Normale Supérieure.

[12] Francois Delor and Michel Hubert. 2000. Revisiting the concept of 'vulnerability". Social Science & Medicine, vol. 50, no. 11, pp. 1557–1570. doi: 10.1016/S0277-9536(99)00465-7.

[13] Catriona Mackenzie. 2016. Vulnerability, Needs and Moral Obligation. in Vulnerability, Autonomy, and Applied Ethics, Routledge. pp. 89–106.

[14] Georg Frerks and Stephen Bender. 2013. Conclusion: Vulnerability Analysis as a Means of Strengthening Policy Formulation and Policy Practice. in Mapping Vulnerability : Disasters, Development and People, 1st ed., London: Routledge. pp. 194–205. doi: 10.4324/9781849771924.

[15] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (Text with EEA relevance).

[16] Council Directive 92/85/EEC of 19 October 1992 on the introduction of measures to encourage improvements in the safety and health at work of pregnant workers and workers who have recently given birth or are breastfeeding (tenth individual Directive within the meaning of Article 16 (1) of Directive 89/391/EEC).

[17] Regulation (EU) No 540/2014 of the European Parliament and of the Council of 16 April 2014 on the sound level of motor vehicles and of replacement silencing systems, and amending Directive 2007/46/EC and repealing Directive 70/157/EEC. (Text with EEA relevance).

[18] Natali Helberger, Martijn Sax, Joanna Strycharz, and Hans-W. Micklitz. 2022. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. Journal of Consumer Policy, vol. 45, no. 2, pp. 175–200, doi: 10.1007/s10603-021-09500-5.

[19] Gianclaudio Malgieri and Jędrzej Niklas. 2020. Vulnerable data subjects. Computer Law & Security Review, vol. 37, pp. 1–16. doi: 10.1016/j.clsr.2020.105415.

[20] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

[21] Gianclaudio Malgieri. 2024. Human vulnerability in the EU Artificial Intelligence Act. OUPblog. Accessed: Sep. 05, 2024. Available: https://blog.oup.com/2024/05/human-vulnerability-in-the-eu-artificial-intelligence-act/

[22] Joel Anderson and Axel Honneth. 2005. Autonomy, Vulnerability, Recognition, and Justice. in Autonomy and the challenges to liberalism: New essays, Cambridge: Cambridge University Press. pp. 127–149.

[23] Robert E. Goodin. 1985. Protecting the Vulnerable: A Re-Analysis of Our Social Responsibilities. University of Chicago Press.

[24] Erin Gilson. 2011. Vulnerability, Ignorance, and Oppression. Hypatia, vol. 26, no. 2, pp. 308–332, 2011, doi: 10.1111/j.1527-2001.2010.01158.x.

[25] Catriona Mackenzie. 2013. The Importance of Relational Autonomy and Capabilities for an Ethics of Vulnerability. in Vulnerability: New Essays in Ethics and Feminist Philosophy, C. Mackenzie, W. Rogers, and S. Dodds, Eds., Oxford University Press. doi: 10.1093/acprof:oso/9780199316649.003.0002.

[26] Javier de la Torre. 2023. Vulnerability: The Human Depth of a Principle of Bioethics. Revista Iberoamericana de Bioética, vol. 21, pp. 1–13.

[27] Martha Albertson Fineman. 2008. The vulnerable subject: anchoring equality in the human condition. in Transcending the Boundaries of Law, 1st ed., Routledge-Cavendish. pp. 1–24. doi: 10.4324/9780203848531-26.

[28] Martha Albertson Fineman. 2010. The Vulnerable Subject and the Responsive State. Emory Law Journal, vol. 60, no. 2, pp. 251–275.

[29] Catriona Mackenzie, Wendy Rogers, Susan Dodds. 2013. Introduction: What Is Vulnerability, and Why Does It Matter for Moral Theory?. in Vulnerability: New Essays in Ethics and Feminist Philosophy, Oxford University Press. doi: 10.1093/acprof:oso/9780199316649.003.0001.

[30] Susan Dodds. 2013. Dependence, Care, and Vulnerability. in Vulnerability: New Essays in Ethics and Feminist Philosophy, Oxford University Press. doi: 10.1093/acprof:oso/9780199316649.003.0008.

[31] Robert E. Goodin. 1985. Vulnerabilities and Responsibilities: An Ethical Defense of the Welfare State/ American Political Science Review, vol. 79, no. 3, pp. 775–787. doi: 10.2307/1956843.

[32] Sandra Wachter. 2024. Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond.Yale Journal of Law & Technology, vol. 26, no. 3, pp. 671–718.

[33] Alessandro Mantelero. 2024. The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. Computer Law & Security Review, vol. 54, p. 106020, Sep. 2024, doi: 10.1016/j.clsr.2024.106020.

[34] Raphaël Gellert. 2021. The role of the risk-based approach in the General Data Protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?. Journal of Ethics and Legal Technologies, vol. 3, no. 11/2021, pp. 15–33. doi: 10.14658/pupj-JELT- 2021-2-2.

[35] Kristiina Brunila and Leena-Maija Rossi. 2018. Identity politics, the ethos of vulnerability, and education. Educational Philosophy and Theory, vol. 50, no. 3, pp. 287–298. doi: 10.1080/00131857.2017.1343115.

[36] Mary Bernstein. 2005. Identity Politics. Annual Review of Sociology, vol. 31, pp. 47–74, 2005.

[37] Kate Brown. 2015. Making sense of vulnerability. in Vulnerability and Young People: Care and Social Control in Policy and Practice, 1st ed., Bristol University Press. doi: 10.46692/9781447318194.

[38] Bige Saatcioglu and Canan Corus. 2015. An inclusive approach to consumer vulnerability: Exploring the contributions of intersectionality. in Consumer Vulnerability, Routledge.

[39] Florencia Luna. 2009. Elucidating the Concept of Vulnerability: Layers Not Labels," International Journal of Feminist Approaches to Bioethics, vol. 2, no. 1, pp. 121–139.

[40] Jörn Birkmann and Ben Wisner. 2005. Measuring the un-measurable: the challenge of vulnerability; report of the Second Meeting of the UNU-EHS Expert Working Group on Measuring Vulnerability. Bonn, Germany. in Studies Of the University: Research, Counsel, Education, no. No. 5. Bonn: UNU-EHS, 2006.

[41] Alessandro Mantelero. 2022. Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI. Information Technology and Law Series. vol. 36. The Hague: T.M.C. Asser Press. doi: 10.1007/978-94-6265-531-7

[42] Janneke Gerards and Frederik Zuiderveen Borgesius. 2020. Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence. SSRN Journal. doi: 10.2139/ssrn.3723873.

[43] Christie M. Gressel, Tarek Rashed, Laura Aswati Maciuika, Srividya Sheshadri, Christopher Coley, Sreeram Kongeseri, Rao R Bhavani. 2020. Vulnerability mapping: A conceptual framework towards a context-based approach to women's empowerment. World Development Perspectives, vol. 20, p. 100245. doi: 10.1016/j.wdp.2020.100245.

[44] Florencia Luna. 2019. Identifying and evaluating layers of vulnerability – a way forward. Developing World Bioethics, vol. 19, no. 2, Art. no. 2. doi: 10.1111/dewb.12206.

[45] European Commission. 2016. Consumer vulnerability across key markets in the European Union. European Commission, Brussels, 2013 86 05 EAHC 2013/CP/08, 2016.

[46] Eleni Kaprou. 2020. The legal definition of 'vulnerable' consumers in the UCPD: Benefits and limitations of a focus on personal attributes. in Vulnerable Consumers and the Law, Routledge, 2020.

[47] OECD. 2023. Consumer vulnerability in the digital age. OECD Publishing, Paris, 355. doi: 10.1787/4d013cc5-en.

[48] Sofia Ranchordas. 2021. Empathy in the Digital Administrative State. SSRN Journal, pp. 1341–1389. doi: 10.2139/ssrn.3946487.

[49] Sofia Ranchordas and Luisa Scarcella. 2021. Automated Government for Vulnerable Citizens: Intermediating Rights. SSRN Journal. doi: 10.2139/ssrn.3938032.

[50] Sofia Ranchordas and Malou Beck. 2023. Vulnerability in Kaufmann, Mareille and Mork Lomell, Heidi (Eds), Handbook on Digital Criminology. Oct. 09, 2023, Rochester, NY: 4596689. doi: 10.2139/ssrn.4596689.

[51] Charter of Fundamental Rights of the European Union. 2012. Official Journal of the European Union.

[52] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.).

[53] European Commission. 2022. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). COM(2022) 212 final, Accessed May 9 2025. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri$=$COM:2022:212:FIN

[54] UN Committee on the Rights of the Child. 2021. General Comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25.

[55] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance).

[56] Sonia K. Katyal and Jessica Y. Jung. 2022. The Gender Panopticon: AI, Gender, and Design Justice. UCLA L. Rev., vol. 68, no. 3, pp. 692–785.

[57] Sinead O'Connor and Helen Liu. 2024. Gender bias perpetuation and mitigation in AI technologies: challenges and opportunities. AI & Soc, vol. 39, no. 4, pp. 2045–2057. doi: 10.1007/s00146-023-01675-4.

[58] Pablo Cerezo Martínez, Alejandro Nicolás Sánchez, and Francisco J. Castro-Toledo, 2024. Discriminatory bias (and how to prevent it) in the European Union: a review of the ethical and regulatory framework for artificial intelligence. Preprint, pp. 1–24.

[59] Raphaële Xenidis. 2020. Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. Maastricht Journal of European and Comparative Law, vol. 27, no. 6, pp. 736–758. doi: 10.1177/1023263X20982173.

[60] Yiran Yang, Frederik Zuiderveen Borgesius, Pascal Beckers, and Evelien Brouwer. 2024. Automated Decision-making and Artificial Intelligence at European Borders and Their Risks for Human Rights. Social Science Research Network, Rochester, NY: 4790619. doi: 10.2139/ssrn.4790619.

[61] Nomisha Kurian. 2024. 'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models. Learning, Media and Technology, pp. 1–14. doi: 10.1080/17439884.2024.2367052.

[62] Simone van der Hof. 2016. I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. Wis. Int'l L.J., vol. 34. Pp. 410-445

[63] Li-Ru Hsu and Simone van der Hof. 2023. Fostering Inclusivity for Children with Intellectual Disabilities through Data Protection by Design. European Journal of Law and Technology, vol. 14, no. 3.

[64] Alessandro Mantelero. 2017. Chapter 8 From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. in Group Privacy New Challenges of Data Technologies, vol. 126, in Philosophical Studies Series, vol. 126. , Cham, Switzerland: Springer International Publishing AG. pp. 139–159.

[65] Robert Wolfe and Alexis Hiniker. 2024. Expertise Fog on the GPT Store: Deceptive Design Patterns in User-Facing Generative AI. DDPCHI'24: Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practice.

[66] Gilly Dosovitsky, Blanca S. Pineda, Nicholas C. Jacobson, Cyrus Chang, and Eduardo L. Bunge. 2020. Artificial Intelligence Chatbot for Depression: Descriptive Study of Usage. JMIR Formative Research, vol. 4, no. 11, p. e17065. doi: 10.2196/17065.

[67] Sandra Wachter, Brendt Mittelstadt, and Chris Russell. 2021. Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. Computer Law & Security Review, vol. 41, p. 105567. doi: 10.1016/j.clsr.2021.105567.

[68] Elodie Boublil. 2018. The Ethics of Vulnerability and the Phenomenology of Interdependency. Journal of the British Society for Phenomenology. Vol. 49. Pp. 183-192. doi: 10.1080/00071773.2018.1434952

[69] Martha Albertson Fineman. 2022. Rights, Resilience, and Responsibility. SSRN Journal. doi: 10.2139/ssrn.4104731.

[70] Martha Albertson Fineman. 2017. Vulnerability and Inevitable Inequality. Oslo Law Review, vol. 4, no. 3, pp. 133–149, Dec. 2017, doi: 10.18261/issn.2387-3299-2017-03-02.

[71] United Nations. 1999. Convention on the Rights of the Child.

[72] Sabine Andresen. 2014. Childhood Vulnerability: Systematic, Structural, and Individual Dimensions. Child Ind Res, vol. 7, no. 4, pp. 699–713, Dec. 2014, doi: 10.1007/s12187-014-9248-4.

[73] Margot E. Kaminski and Gianclaudio Malgieri. 2021. Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations," International Data Privacy Law, pp. 125–144. doi: 10.2139/ssrn.3456224.

[74] Margot E. Kaminski. 2018. Binary governance: Lessons from the GDPR's approach to algorithmic accountability. S. Cal. L. Rev., vol. 92, p. 1529-1616.

[75] Inga Ulnicane. 2024. Intersectionality in Artificial Intelligence: Framing Concerns and Recommendations for Action. Social Inclusion, vol. 12, no. 0. doi: 10.17645/si.7543.

[76] Giacomo Figà-Talamanca. 2024. Digitally Scaffolded Vulnerability: Facebook's Recommender System as an Affective Scaffold and a Tool for Mind Invasion. Topoi, 43, 631–643. doi: https://doi.org/10.1007/s11245-024-10051-w

[77] Federico Galli and Claudio Novelli. The Many Meanings of Vulnerability in the AI Act and the One Missing. BioLaw Journal. pp. 53-71.

[78] European Commission. 2025. Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final.

[79] Daniella DiPaola and Ryan Calo. 2024 Socio-digital vulnerability. SSRN Scholarly Paper. Doi: http://dx.doi.org/10.2139/ssrn.4686874

[80] Maria-Lucia Rebrean and Gianclaudio Malgieri. 2025. On administrative and surveillance vulnerability and the digital government in the EU. In Data Retention in Europe and beyond: Law and Policy in the Aftermath of an Invalidated Directive. Oxford Academic. pp. 455-470. doi: https://doi.org/10.1093/9780191998980.003.002

[81] Lourdes Peroni and Alexandra Timmer. 2013. 'Vulnerable groups: The promise of an emerging concept in European Human Rights Convention law'. International Journal of Constitutional Law. vol. 11 pp. 1056–1085,

[82] Indira Boutier. 2024. 'Understanding Vulnerability through the Eyes of the European Court of Human Rights' Jurisprudence: Challenges and Responses' Peace

Human Rights Governance, vol. 8 , pp. 27-52.
[83] Sue Anne Teo. 2023. Human dignity and AI: Mapping the contours and utility of human dignity in addressing challenges presented by AI. Law, Innovation and Technology, 15(1), 241-279. doi:
[84] Sue Anne Teo. 2025. 'Artificial intelligence, human vulnerability and multi-level resilience'. Computer Law and Security Review, vol. 57, Advance online publication doi:. https://doi.org/10.1016/j.clsr.2025.106134
[85] European Convention on Human Rights. 1950. Council of Europe.
[86] Yochay Nadan and Jill Korbin. 2018. Cultural Context, Intersectionality, and Child Vulnerability. Childhood Vulnerability, vol. 1, no. 1, pp. 5–14. doi: 10.1007/s41255-019-00003-7.