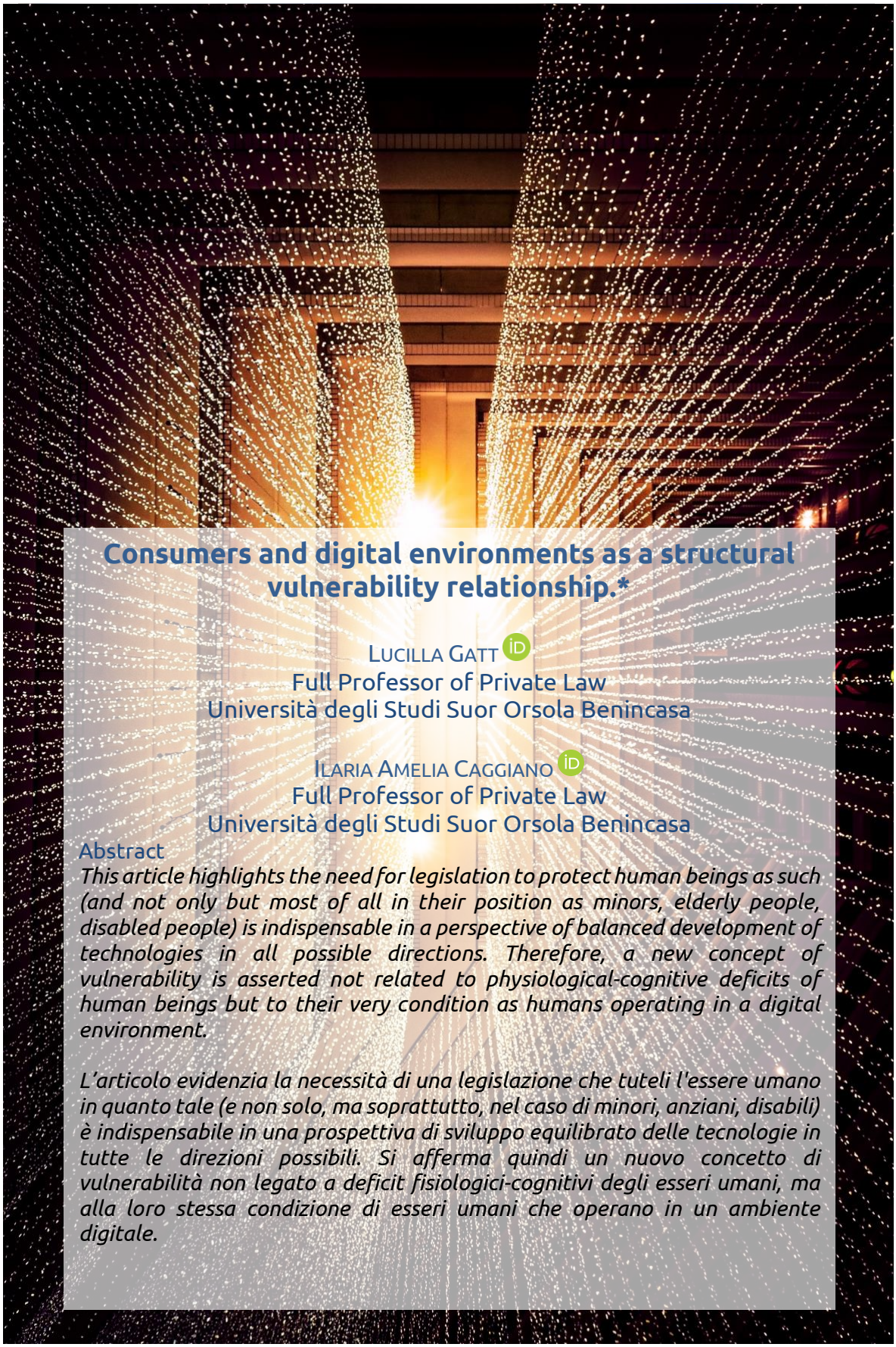
Gatt L, Caggiano I, 'Consumers and Digital Environments as a Structural Vulnerability Relationship ' (2022) 2 EJPLT, 8-16.
DOI: https://doi.org/10.57230/EJPLT222LGIAC

EJPLT
ISSN 2704-8012



Consumers and digital environments as a structural vulnerability relationship.*

Lucilla Gatt
Full Professor of Private Law
Università degli Studi Suor Orsola Benincasa

Ilaria Amelia Caggiano
Full Professor of Private Law
Università degli Studi Suor Orsola Benincasa

Abstract

This article highlights the need for legislation to protect human beings as such (and not only but most of all in their position as minors, elderly people, disabled people) is indispensable in a perspective of balanced development of technologies in all possible directions. Therefore, a new concept of vulnerability is asserted not related to physiological-cognitive deficits of human beings but to their very condition as humans operating in a digital environment.

L'articolo evidenzia la necessità di una legislazione che tuteli l'essere umano in quanto tale (e non solo, ma soprattutto, nel caso di minori, anziani, disabili) è indispensabile in una prospettiva di sviluppo equilibrato delle tecnologie in tutte le direzioni possibili. Si afferma quindi un nuovo concetto di vulnerabilità non legato a deficit fisiologici-cognitivi degli esseri umani, ma alla loro stessa condizione di esseri umani che operano in un ambiente digitale.

* The author of paragraphs 1 to 5 is Lucilla Gatt, Full Professor of Private Law and Director of the Research Centre of European Private Law; the author of paragraphs 6 and 7 is Ilaria Amelia Caggiano, Full Professor of Private Law and Vice-Director of the Research Centre of European Private Law.

Keywords: human being; new technologies; new vulnerabilities; minors; ethical space; education.

1. The concept of relational vulnerability with special regard to the technological environment.

In the legal field, vulnerability is a relational concept.

It is a multidimensional and correlated condition, no longer a status linked to old age, minor age, female gender or disability conditions. In the current legal framework at national and international level, vulnerability can be considered to have acquired a broader meaning.

It includes all living entities – from humans to animals or plants (although this aspect is not considered in this document) – when they operate in contexts where other actors are more powerful for various reasons: social, economic or cultural, physical strength, possession of weapons and, last but not least, technological gap.

This means an imbalance in starting positions, which determine someone's vulnerability to someone else. This condition, in turn, means that someone is capable of profiting someone else or, more dramatically, causing them pain or death.

Having identified the condition of vulnerability in these terms, it seems plausible to state that:

1) the abuse of a person in a position of greater power/strength to the detriment of another person is unjust.

2) the subject who is in a weak position – i.e., the vulnerable subject – must be protected from any abuse of power/strength by the other subject.

2. The role of law in the vulnerability context.

Assuming a historical perspective with Europe and neighboring countries at the center, it can be seen how these conclusions, although currently (apparently) shared when it comes to national and international Western charters on fundamental rights, have not always been applied in economic practice and legal. In other words, for a relatively short time the idea has penetrated Western culture that being holders of greater physical, intellectual, cultural, and economic strength does not authorize behaviors of oppression of various kinds on who or what cannot react with of equal importance and

intensity.

The word 'vulnerability' (from the Latin 'vulnerare', to wound) literally means 'likely to be injured'. Figuratively, it refers to the precariousness of a condition marked by the possibility of violation and limitation, often defined by different degrees of weakness, dependence, lack of protection. Cicero spoke of three realities susceptible to being injured: life, reputation and health. Similarly, contemporary philosophy emphasizes different meanings of vulnerability: physical, psychological, spiritual, political and legal. The «Declaration of Barcelona» of 1998 represents an important event in the promotion of the category of vulnerability, in view of its possible public legitimization, so to speak, in the field of bioethics. The Declaration was signed by a group of twenty-two European scholars and represents the result of three years of study promoted by the European Commission. [1] It is structured around four new principles, of which the principle of vulnerability is the innovative principle. In fact, the Barcelona principles represent, taken together, a critique and a rather conspicuous alternative to the four principles of North American bioethics: autonomy, non-maleficence, beneficence and justice (W. T. Reich, 2001).[2]

Conversely, the position of greater strength translates into greater responsibility to who or what is in a different position. This trend can be seen in European and not only European policies of the green deal and human-centered artificial intelligence.

This attests to an evolution in the European culture of the concept of vulnerability in the sense of a transition of the vulnerable entity (that is to say: weaker) from an object of oppression to a subject to be protected. That said, the tools that can be used to counter the abuse and to protect the vulnerable subject from abuse are of a preventive or repressive nature. In both cases, the law comes into play, i.e., a mandatory regulatory apparatus with adequate prescriptions and corrective tools. These norms make illegal the abuse to the detriment of the vulnerable, which otherwise would only possibly be ethically unacceptable (unjust, in fact).

Because of this possible prospect, it was decided to develop a research and teaching project on the vulnerability of human beings in relation to digital technology[3]. This is one of the areas in which the relationship of vulnerability has developed, understood as a relationship of fragility of one subject with

[1] The «Declaration of Barcelona» of 1998 has been developed within the Bio-Med II research project (1995-1998), founded by the EU Commission. The results of the Bio-Med II EU research project have been published: P Kemp, J Rendtorff, NM Johansen, Bioethics and biolaw. Vol. I-II. (Rhodos international Publishers 2000).

[2] W T Reich, 'Prendersi cura dei vulnerabili: il punto di incontro tra etica secolare ed etica religiosa nel mondo pluralistico' (2002) 3, Annali di Studi Religiosi, 71-86.

About the basic principles for European bioethics: P Kemp JD Rendtorff, 'The Barcelona Declaration – Towards an Integrated Approach to Basic ethical principles' (2008) 2, Synthesis Philosophica, 239 – 251; JD Rendtorff, 'Basic ethical principles in European bioethics and biolaw: autonomy, dignity, integrity and vulnerability - Towards a foundation of bioethics and biolaw' (2002) 5, Med Health Care Philos; P Kemp, 'Four ethical principles in biolaw' (2000) 2 Bioethics and Biolaw, 13-22.

About the principles of North American bioethics: TL Beauchamp, JF Childress, Principles of biomedical ethics (Oxford University Press 1979).

[3] The research and teaching project has been developed within the activities of the Jean Monnet Chair 'European Protection Law of Individuals in Relation to New Technologies – PROTECH', held at the University Suor Orsola Benincasa of Naples, faculty of law.

Project website is available at https://www.protech-jeanmonnet.eu

respect to another: (e.g., consumer natural person, on the one hand, platforms – e-commerce or social-network – from the other one). Compared to this relationship, minor age or advanced age or computer illiteracy or single disability are not the cause of vulnerability but can represent an aggravating factor.

3. The phases of relational vulnerability discovery.

The analysis started from the focus on vulnerability as a concept that can be elaborated, following the following phases:

a) to map and analyze with a multidisciplinary method the most evident cases of vulnerability aka 'difference of positions' in the various sectors such as, for example, human rights violations in dictatorial governments; the forced occupation of territories; unfair terms in consumer contract law; the abuse of power in private and public relations; the determination of the will of others through the undeclared and unauthorized use of technological tools; the abusive treatment of personal data and the like.

b) extrapolate the recurring weaknesses from these scenarios.

Considering each element of weakness as a value to be protected, we can highlight the values to be included in the mandatory regulatory frameworks to ensure that protection against vulnerabilities is guaranteed at the macro level.

In summary, vulnerability is an indicator of greater weakness on one side of the relationship. This weakness must be considered a value, i.e. an asset to be protected through the adoption of adequate regulations.

4. The technological vulnerability.

This scenario and the consequent need for protective legislation occurs above all in the relationship between human beings and the digital environment in all its possible articulations.

In the technological habitat (for example: e-commerce platforms) a subject can act in an unfamiliar context that can be known or simply more comfortable or familiar to others for various reasons (digital divide, minor/old age, asymmetry of bargaining or information power). But in this large category of vulnerable subjects we also include human embryos, which are a crucial example of exposure to the risk of harm (alias vulnerability) because they do not act but are created aborigine in a technological and highly manipulated environment without their consent.

Ultimately, in digital habitats the subjects that can be qualified as more vulnerable are:

– Those concerned with particular regard to Minors and the Elderly;

– Consumers with particular regard to Minors and the Elderly;

– Embryos, unborn children, new life forms created in the laboratory.

It is necessary to highlight or, better, to promote a protective approach in existing national and international legislation (data protection, consumer protection, embryo protection), which regulates the relationship between

individuals and technologies.

Finally, also to increase students' awareness of vulnerability as a value to be protected, we also consider their condition as vulnerable subjects, in relation to teaching staff. This assumption can be the basis of a new integrated educational model (online and offline) with a high level of accessibility and usability in a global scenario.

The crucial point lies in the determination of a concept of vulnerability that is not linked to specific physical or psychological disabilities but is identified in the relationship between the physical person and the technological environment in which he/she operates (Gatt L., 2022)[4].

5. The ethical space as an intermediation tool in the relationship of vulnerability.

Having taken note of the ontological vulnerability of human beings – in general – with respect to digital technology structures, it should be emphasized that the law alone is not sufficient to reconcile the interests at stake and to achieve objectives of effective protection.

The rules must express a direction, choosing to protect weakness as a value but they must also prepare concrete tools by foreseeing them. Among these, a very valid tool is that of the Ethical Space which translates into an entity of various kinds, adaptable to the context in which it is called to operate.

With regard to the 'educational fact', i.e., the teacher-student training relationship, it is important that it takes place in suitable places and with suitable means to guarantee the weak subject of the relationship total and equal access to the educational path.

The physical space where training takes place must be built and designed to compensate for this disparity of positions (for example: digital training requires adequate tools and equal accessibility to them as well as human resources dedicated to training and the required support).

This principle of the organization and structuring of physical and digital space according to the maximum usability, accessibility and effective utility for the weak subject is also valid in the relationship between student and teacher as well as consumer and entrepreneur and, above all, between citizen and State.

Think of the issue of the digital identity needed to access many if not all public services. Also, this relationship between natural person and public subject requires the adoption and construction of ethical spaces (e.g., intermediation stations with dedicated human resources; chats with human operators; clear and transparent information; loyal behavior on the part of the public administration).

The conscious use of places, of real and virtual spaces together with the involvement of human resources prepared to guarantee represents the real

[4] L Gatt, 'Legal anthropocentrism between nature and technology: the new vulnerability of human beings' (2022) 1 EJPLT, 15-26. DOI: https://doi.org/10.57230/EJPLT221LG

challenge for a real transition to digital for all those who find themselves in a position of vulnerability.

6. A special category of vulnerable individuals: Minors, and the case of data protection.

When looking at the existing law, one might consider if it protects technological vulnerability. To analyze this aspect, we will consider European data protection regulation (GDPR, EU Reg. 2016/679), which is a case where vulnerability towards technology, although not being qualified in such a manner, is taken into consideration for regulating personal data of children.

Minors are legally vulnerable individuals, as already foreseen in other areas of law (ex. Family, Contract, Immigration Law).

In the digital world, they become, indeed, doubly vulnerable: they are not fully aware of themselves and the perceivable world and for this reason they are already legally protected in various context (subjective vulnerability); in addition, they are more exposed to unknown or not perceivable risks arising from the digital environment (technological vulnerability).

Probably for this reason, minors are the only category of vulnerable subjects expressly foreseen by the GDPR, in various provisions, either only as subjective vulnerable persons or as also technologically vulnerable ones.

Whereas (38) of the GDPR identifies reasons why children are considered vulnerable persons and therefore merit specific protection, as well as the principal areas where processing of personal data needs to be under attention: *« […] they may be less aware of the risks, consequences and safeguards concerned and their rights […]. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. [..]».* The reference made in whereas 38 to creation of personality or using profiles implicitly refers to the digital world. More specifically, the EDPB Guidelines on the targeting of social media users[5] focuses on the potential adverse impact of targeting, which « […] *can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development*».

The Guidelines refer to risks which are known in social studies as the *filter Bubble* phenomenon, where during the web navigation algorithms select information that a profiled user would like to see, based on past information about him/her, and past click-behavior and search history. As a result, users are not used to information that disagrees with their viewpoints, effectively isolating them in cultural or ideological bubbles. For minors, this means that they do not have the chance to develop critical viewpoints based on diverse, even conflicting, information.

For protecting vulnerability, the GDPR adopts a regulatory technique based on the general principles and the general obligations already in charge of the

[5] Guideline 8/2020 on the targeting of social media users, adopted on 13 April 2021. Available online at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en

data controllers, which they must implement, through decisions and processes in their business or institutional activity (*e.g.*, Data protection by design and by default). Except spare cases, one would not find specific rules addressing vulnerability, whilist not-binding recommendations are variously provided for.

The GDPR reinforces what is already foreseen on a general basis as for rights and interests of minors: in terms of recommendation regarding the Right to erasure ('right to be forgotten') (art. 17), Whereas 65 recommends guaranteeing in any case the right to erasure if the consent has been given when the subject was minor.

The balancing test that the data controller must undertake between legitimate interest and rights and freedom of the data subject must be particularly cautious when he/she is a minor (art. 6, §1, *f)* GDPR).

More specifically, protection of minors as technologically vulnerable subjects is devised through the general obligations of the data controller, and recommendations to him/her.

Consideration of minors as technologically vulnerable subjects can specify the Data-protection-by-design-principle, which is referred to data processing in general (Art. 25). Whereas 71, states: *Profiling ... should not concern a child*. According to *soft law* (WP 29, Guidelines on Automated individual decision-making and Profiling) [6] this prohibition must be considered only as a recommendation, as well as the one regarding apps on smart devices (WP 29, Opinion 02/2013) [7] : App developers must '[…] refrain from processing children's data for behavioral advertising purposes, either directly or indirectly […]'.

If the data processing concerns vulnerable data subjects and/ or the digital environments, the data controller may be obliged to conduct a Data Processing Impact Assessment before starting or to continue the processing. Soft law (WP29 Guidelines) identifies some specific criteria in this regard, including evaluation or scoring, profiling; Automated-decision making with legal or similar significant effect; Data processed on a large scale; Data concerning vulnerable data subjects (minors, mentally ill persons, asylum seekers, or the elderly, patients, etc.).[8]

The DPIA is required if at least two of these criteria are met, but – taking into account the circumstances – the data controller can decide to conduct a DPIA even if only one of the above criteria is met.

Binding provisions regulate minors' decision, both as for the information to be provided (art. 12), and for the consent itself (art. 8). In this last case, GDPR takes into consideration technological vulnerability of minors in the information society services, as a context within which the minor operates

[6] WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018. Available online at https://ec.europa.eu/newsroom/article29/items/612053

[7] WP29, Opinion 02/2013 on apps on smart devices, 00461/13/EN WP 202, adopted on 27 February 2013. Available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[8] WP 29 Guidelines on Data Protection Impact Assessment (DPIA) 17/EN, WP 248 rev.01, Adopted on 4 April 2017. Available online at https://ec.europa.eu/newsroom/article29/items/611236/en

more widely and freely and fixes an age threshold (16 years) to give consent to the data processing as a legal basis.

Following the waiver allowed by GDPR, a number of Member States, among which there is Italy, has lowered this threshold age, thus altering in principle the harmonization of markets.

7. Some considerations on the current regulation of minors' vulnerability in the digital environment.

The regulatory framework depicted on the regulation minors' data takes into account their technological vulnerability by charging the data controller with evaluations to carry out and decision to take, or by fixing more specific rules.

At this point, some considerations on the state of the art may be done.

As for the privacy consent of minors in the digital environment, in our view, diversification of the age threshold among Member States is a collateral issue in terms of relevance if one regards the role of the rule of consent in the operating practice.

One must recognize that the impact of the rule on minors' consent in the digital environment is sensibly weak for a number of reasons:

(1) The scope of the rule is the consent as a legal basis for data processing, which means that it is relevant for those processing of data not included in the performance of the contracts and in the legitimate interest (e.g., only behavioural advertising, and, profiling, according to the evaluations of the controller);

(2) Therefore, access to platforms is regulated by contract rules. The social networks more desirable by minors fix low threshold ages for contracting, adopting same rules in different countries (12 years), probably relying on the overall validity of the contract, since subscription to social networks has to be considered as a means for expressing freedom and personality;

(3) On the privacy by design perspective, social networks (*e.g.,* Tik-tok, privacy policy) provide for different age groups (13-15; 16-17) for the share and third parties access functions.

As for the consent profile, wherever it is contractual consent or privacy consent (regulated by art. 8 GDPR), the crucial point for protecting children acting in the digital world is to verify their age. Given the absence of expressed rules, as well as the flawless of verification mechanisms currently activated (*e.g.*, one-choice option) and traditionally considered (*e.g.*, id card, parents' payment card), nowadays it is more than easy for a child to create a fake profile, declaring an older age. This expedient can make the law virtually ineffective, if not supported by different technologies enabling verification (id recognition, blockchain and / or smart contracts), which, however, bring other data protection issues, or written-alike mechanisms of contract conclusion (*e.g.*, qualified electronic signature), which has been historically an instrument of protection of vulnerable parties.

On the side of the obligations and the compliance processes in charge of controllers, here *ex post* remedies, Supervisor's activities and deterrence of

sanctions are the institutional tools, even if not capillary, to control data processing of minors and protect their vulnerability.