# AI Act and Individual Rights: A Juridical and Technical Perspective

Costanza Alfieri[1,†], Francesca Caroccia[1,†] and Paola Inverardi[1,*,†]

[1] *Università degli Studi dell'Aquila, L'Aquila, Italy*

**Abstract**

In April 2021, the EU Commission published a new proposal, laying down harmonized rules on Artificial Intelligence (AI Act). In the Commission's view, such a harmonized solution has the double role of strengthening the internal market and remaining competitive with other regions of the world while providing legal certainty and adequate remedies to consumers and producers. In this contribution, we present an analysis of the AI Act by addressing the problem of liability and respect of individual rights. The analysis shows that the AI Act takes into consideration the social dimension of the risks, whereas the hypothesis of a concrete breech of individual rights is neglected. In this context, we propose both technical and juridical solutions which are based on the idea of improving human-machine interaction. The technical solution aims at empowering the user when interacting with the digital world, whereas the juridical solutions provide a legal ground both for supporting the technical proposal and for guaranteeing augmented interaction between machine and the users.

**Keywords**

AI Act, Autonomous System, Liability, Human-machine Interaction

## 1. Introduction

### 1.1. AI Act: Balancing Technological Competitiveness and Fundamental Rights.

In April 2021, the EU Commission published a proposal, laying down harmonized rules on Artificial Intelligence (AI).

The Commission's initiative has been the first ever attempt to build a specific EU legal framework, to regulate (some aspects of) the use and commercialization of AI Systems. Until now, the question was subject to a wide range of national and supranational law and principles, on singular and specific aspects: such a harmonized solution has a crucial importance, not only to strengthen the internal market and remain competitive with other regions of the world, but also to provide legal certainty and adequate remedies to consumers and producers. In the Commission's view, the legislative intervention should ensure that European companies

*IAIL 2022 - Imaging the AI Landscape after the AI Act, 13th of June 2022, Amsterdam, Netherlands*

[*] Corresponding author.

[†] All Authors have read and agreed to the published version of the manuscript. F. Caroccia is responsible for par. 1, 1.1, 1.2, 2, 2.1, 2.2, 2.3, 3.2, 3.3; C. Alfieri and P. Inverardi are responsible for par. 3, 3.1, 4.

costanza.alfieri@student.univaq.it (C. Alfieri); francesca.caroccia@univaq.it (F. Caroccia); paola.inverardi@univaq.it (P. Inverardi)

0000-0002-5082-3844 (C. Alfieri); 0000-0002-2328-9527 (F. Caroccia); 0000-0001-6734-1318 (P. Inverardi)

CEUR Workshop Proceedings (CEUR-WS.org)

maintain competitive advantages and technological leadership but, at the same time, “that people can trust the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights”[1]. The respect of fundamental rights, protected both under the Treaties of the European Union and the EU Charter of Fundamental Rights, is a key-theme, when AI technologies are concerned. Most notably, it is underlined that AI systems may affect the right to non-discrimination, freedom of expression, human dignity, privacy. In this regards, it is not useless to recall the necessity of the proportionality test: any interference with a Charter right needs to be examined as to whether the given legitimate aim could not be obtained by other means that interfere less with the right guaranteed. Concerning new technologies, the ECHR expressly observed that States should “strike a right balance” between protecting fundamental rights and developing new technologies[2].

The new rules should be applied to a wide range of actors: as usual, to users of AI systems located in the EU, to providers of AI systems established within the EU or placing AI systems on the EU market, but also to users and providers of AI systems located in a third country, where the output produced by those systems is used in the EU. Moreover, the EU’s law is expected to be one of the first of the world on AI technology, setting a global standard for emulation by other jurisdictions [1]. This entails, inter alia, the opportunity and responsibility of proposing a “European human-centered model” [2] of interacting with AI that is, a model found “in respect for human dignity, in which the human being enjoys a unique and inalienable moral status” [3].

## 1.2. The “Risk-based Approach”: Liability Rules vs. Accountability Rules.

As it is known, the Commission proposal is focused on a “risk-based” approach, according which AI systems are classified on the basis of the level of risk they represent for fundamental rights. In this perspective, AI systems are categorized as “unacceptable” risks systems (prohibited), “high-risk” systems (authorized, but subject to requirements and certifications to access to the EU market – following a premarket conformity regime), “limited risk” systems (subject to very light transparency obligations: codes of conduct and similar), “low or minimal” risk systems. Some AI systems presenting limited risks (such as systems that interacts with humans, i.e. chatbots) would be subject to a limited set of specific transparency obligations (see Figure 1).

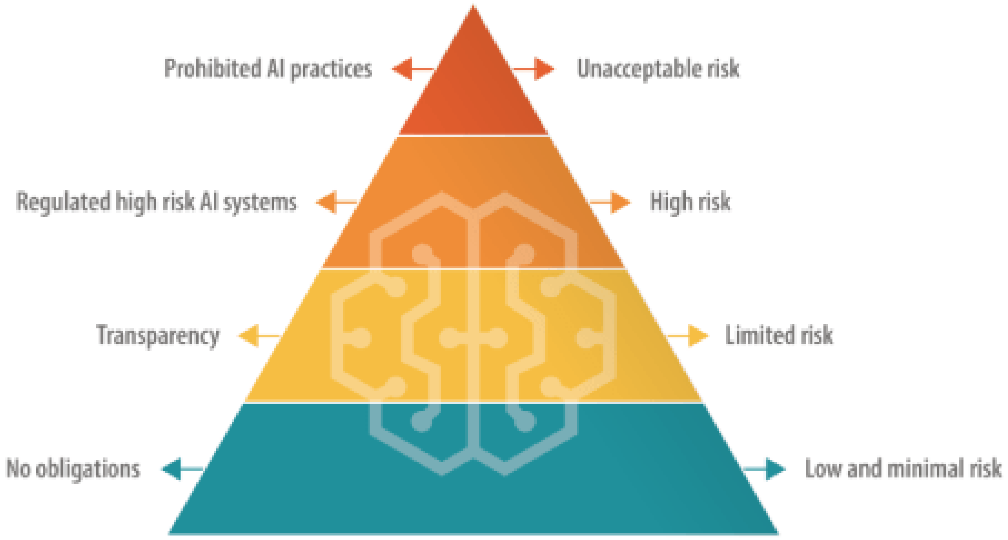
By this way, a minimalist regulatory approach is designed, where legal intervention “is tailored to those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future” [3].

At a national level, the respect of the new rules should be ensured by market surveillance authorities, which would be responsible for assessing operators’ compliance with the requirements for high-risk systems (pre-market assessment). At a central level, an European Artificial Intelligence Board is previewed, to ensure harmonised implementation of the Act and cooperation between national authorities and the Commission.

[1] The EP Resolution on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies (October 20, 2020) specifically recommended to the Commission to propose legislative action balancing opportunities and benefits of AI, with protection of ethical principles.

[2] ECHR, S. and Marper v. the UK, Nos. 30562/04 and 30566/04, 4 December 2008, par. 112

[3] See definition provided by the High-Level Expert Group on AI (glossary section of the Ethics Guidelines for Trustworthy AI).



Data source: European Commission.

**Figure 1:** Pyramid of Risk.

Administrative fines are set out to sanction non-compliance with the AI Act.

This model is not too far from GDPR: it implies a set of norms aimed to evaluate the conduct of the actors (here we refer to the "producers" actors, but in the digital world there are also other actors, the consumers and/or other actors that are no producer and no consumers but may be anyhow impacted by the technology); a governance to guarantee compliance with behavioral rules (national market surveillance authorities or similar); the existence of possible sanctions[4]. It shows to actors how they might act in order to be compliant, on the assumption that producers and users should respect predetermined criteria.

As it was already observed with regards to GDPR, the shift from liability to accountability is evident [2, 4, 5]. In such a new accounting model, the agents are requested to adopt strategies and concrete measures, in order to reduce risks connected with the use of AI. At the same time, they can autonomously determine modes, guarantees and limits of their own conduct, provided that they build a strategy to reduce risks, within the new European legal framework. By this way, producers can pre-determine the level of risk, that allows them to maximize utilities and minimize responsibility. Within this context, liability rules should be called to integrate and complete the system, providing solutions when a damage occurs, despite the respect of prevention measures. Instead, in the AI Act liability rules are completely absent: the Commission merely points out that the proposal has to be complemented by other initiatives that address liability issues related to new technologies (including the revision of product safety legislation)[5]. In other words, the normative focus shifts from the ex post (after the damage) to

[4] European Parliament resolution of 16 February 2017 with recommendations to the Com-mission on Civil Law Rules on Robotics (2015/2103(INL)).

[5] On 30 June 2021, the Commission adopted a proposal for a regulation on general product safety, which would

the ex ante (harms prevention) phase. This is a significant novelty, in the European strategy of AI regulation: even if the previous interventions (as, for example, the European Parliament resolution on Civil Law Rules on Robotics) do not ignore the risk management approach (which was expressly indicated in the mentioned resolution as a strategic tool to reduce risks), they were focused right on liability rules. By this way, the Commission seems to accept the suggestion of adopting prevention policies, enabling companies to quantify the costs of accidents, on the grounds that liability rules fundamentally are instruments to allocate loss, while accountability systems offer effective incentives to risks prevention.

## 2. Some Critical Issues

After its publication, the Commission's proposal received a number of non positive feedback from stakeholders. Most of them called for a major revision of the AI Act, aimed to ensure a better allocation of responsibility, to strength enforcement mechanisms and to foster democratic participation[6].

To achieve those objectives of preserving individual safety and fundamental rights, without overly inhibiting innovation in AI, a "balanced" approach is put in place. However, the Commission seems to fail to translate her intention into concrete and effective action, considering that the regulatory framework is built following criteria of "minimum necessary requirements". It is evident the Commission's concern of preserving the EU's technological competitiveness: the solution adopted promotes the AI development, avoiding the increasing of the costs of AI systems commercialization, "without unduly constraining or hindering technological development" [3]. On the contrary, the question of the consistency with Union values and fundamental rights is clearly declared, but substantially underestimated.

Many experts, indeed, underline that the described approach does not guarantee an adequate level of protection of fundamental rights (and, at the same time, it disadvantages small and medium enterprises, which will not be able to manage the procedural burden imposed by legislation, as the experience of GDPR clearly showed).

### 2.1. The lack of enforcement structures

Accountability, in this context, means "the ability to determine whether a decision was made in accordance with procedural and substantive standards and to hold someone responsible if those standards are not met"[6]. It is considered desirable, if not necessary, for several reasons. Mainly,

- it enables producers to perform the risks assessment process in terms of costs/benefits analysis, ensuring EU competitiveness on global markets;

- it responds to the necessity of avoiding damages caused by hazardous activities, on the assumption that the consequences of this kind of damages could be devastating and impossible to remove (i.e. nuclear disasters).

replace the current General Product Safety Directive and cover product safety of emerging technologies (COM (2021) 346 30.6.2021.

[6] EPRS European Parliamentary Research Service: Artificial intelligence act. Briefing,www.europarl.europa.eu/ReData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf, last accessed 2022/3/25.

But, what happens in case of failure to comply with the requirements, or when a damage is caused, despite the adoption of preventive measures? While the proposal disciplines the preventive phase, it does not answer to the question about the breech of the law [1, 7].

Scholars stress that the AI Act fails to establish effective enforcement structures [8]. The power transferred to Member States in this domain is not sufficient and the experience of GDPR has showed that enforcement by national authorities leads to different levels of protection across the EU, not only due to resources assigned but also to cultural context. Moreover, the weakness of public enforcement is not compensate by private tools. Implementation is essentially left to the self assessment and private control (EPOs) (a kind of voluntary phase), and users (individuals affected by AI systems, civil rights organizations, etc...) have no right to complain to market surveillance authorities or to sue a provider.

More in general, the AI Act does not provide for any individual rights, nor for remedies by which damaged parties could react against failures under the AI Act.

To explain this question, the example of GDPR could still be useful. The GDPR clearly lists both the rights of the data subject (chap. 3, artt. 12-23) and remedies and penalties (artt. 77-84) in case of unlawful conduct, expressly stating, among others, that "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered". In the AI Act, on the contrary, similar rule are lacking: the act does not contain any reference to individuals' rights, does not recognize any right to compensation to damaged users. The legal framework is entirely designed from the companies' perspective [9].

Said otherwise, in this part AI Act only takes into consideration the social dimension of the risks (that is, it prevents and reduce the costs of accidents for the entire society), whereas the hypothesis of a concrete breech of individual rights is neglected (that is, it ignores the question of the allocation of the loss, when an individual is concretely damaged). Yet, "the major concern for any responsibility system is ensuring victim compensation": as Scholars pointed out, "ex ante safety should be decoupled from ex post compensation" [10]. Besides the accountability directives, liability rules have to be taken into consideration, to build an effective responsibility model: accountability and liability rules need to be reciprocally integrated and completed.

Probably, it would be necessary to know the entire regulatory plan conceived by the Commission, in order to express a judgement. As we said, the AI Act is only an element of a complex picture, which includes the revision of the safety legislation[7] (such as the Machinery Regulation and the General Product Safety Directive) in order to develop an ecosystem of trust for AI. It is not a case if two months after, on 30 June 2021, the European Commission published an inception impact assessment for a Directive on "Civil liability - adapting liability rules to the digital age and artificial intelligence". Accountability and liability rules are both necessary to build an efficient system of damage control, since they govern two different moments (ex ante-ex post) of the same problem.

However, it seems that some consideration may be expressed, even at this stage.

[7] See footnote 5

## 2.2. Definition of the risks level and the lack of democracy

Following the proposal, AI systems are classified on the basis of the level of risk they represent for fundamental rights. Critics have been raised on the classification model. As it has been underlined, this way of ex ante linking AI systems to different risk categories does not consider that the level of risk also depends on the context in which a system is deployed and cannot be fully determined in advance. The main consequence is a certain level of legal uncertainty for developers, operators, and users of AI systems [11].

From a different perspective, a strategy is suggested, in order to introduce and ensure for EU citizens a right of consultation and participation in public decision-making on AI, in order to ensure democratic procedures and a better level of protection not only for individual rights, but also for societal interests. Scholars highlight an excessive delegation of regulatory power to private bodies, which may produce a societal harm [8]. Within this context, the concept of "societal interest" (and of societal harm) is considered as distinct from the "individual" or "collective", as it "goes beyond the concern of (the sum of) individuals, but affects society at large". Indeed, societal harms concern to an interest held by society, "going over and above the sum of individual interests" [12]. As it was observed, quite paradoxically, the AI Act succeeds in ignoring the question of societal harms (i.e. environmental harm, voter manipulation etc.), and, at the same time, neglecting individual rights [12].

## 2.3. Ethics guidelines are the best way to protect fundamental rights?

Lastly, the question of the use of ethics. Under the AI Act, high-risk systems would have to comply with both technical and legal obligations, while providers of limited risk systems are simply encouraged to adopt ethical rules. This is necessary to preserve individual safety without inhibiting innovation. Nevertheless, this overlap of juridical (technical/legal requirements) and ethical (codes of conduct) rules is not convincing. The approach is not new. With specific regard to AI, it has been observed that, by 2019, more than 80 Ethical Guidelines have been published on national and international level [13], with the involvement of consumers, other stakeholders and their representative organisations. The same EU Commission in April 2019 published a set of non-binding Ethics guidelines for trustworthy AI, prepared by the Commission's High-Level Expert Group on AI, aimed "to offer guidance on how to foster and secure the development of ethical AI systems in the EU"[8]. However:

1. the civil society's involvement is not in itself a guarantee of fair representation of different interests at stake. A disproportion between the presence and the right balance of different stakeholder's voices has been observed in many expert hearings in terms of AI policies;
2. the existence of a number of codes of ethical rules could encourage the "ethics shopping": the risk is the creation of a market of principles and values, "where private and public actors may shop for the kind of ethics that is best retrofitted to justify their current behaviours" [14];
3. the AI Act does not answer to the question on possible conflicts among different ethical rules/codes of conduct;

[8] Independent High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, April 8 2019

4. empirical experiments show that ethics guidelines has no significant influence on the decision-making of software developers: ethics rules are often considered as “extraneous”, “imposed from institutions outside of the technical community”. Moreover, “where ethics is integrated into institutions, it mainly serves as a marketing strategy” [15];
5. the proposed model has been viewed as an “unlawful delegation of the Commission’s rulemaking power to private bodies” [7] (with all that this implies in terms of lack of transparency and democracy): “ethics guidelines, as well as other concepts of self-governance, may serve to pretend that accountability can be devolved from state authorities and democratic institutions” [16];
6. “minimum risk” does not necessarily means “absence of risk”: also in this case, there is no assurance that a harm may occur, and the AI Act does not provide solutions in this case.

And then again the adoption of codes of conduct is simply “encouraged”. Scholars point out that ethics has a lack of reinforcement mechanisms and deviations from ethics rules has no consequences. If so, there is a gap in the protection of individual rights against concrete harms, as the AI Act does not recognise specific justiciable and/or enforceable rules. In brief, “those impacted by AI systems – sometimes thought of as end-users, data subjects or consumers – have no rights, and almost no role in the AI Act” [17].

## 3. Proposals

The question at stake arises as to whether the described strategy (from liability to accountability, we said) optimises the normative tool, in order to achieve the declared goals (that is, a balance between competitiveness and protection of fundamental rights), or is it possible to imagine other solutions to strength and integrate such a model.

Moreover, it has been showed that the solution of voluntary ethical guidelines still present several limits.

While waiting for a better definition of the EU’s regulatory framework, it is worth understanding if in the current legal context there are ways to design AI systems and their interactions with users in order to improve the degree of fundamental rights protection, answering the call for more “tangible bridges between abstract values and technical implementations” [15].

From the particular perspective of the human dignity, a possible answer lies in a stronger involvement of users, aimed to raise the level of the human-machine interaction.

In [18], the authors affirms that “there is an emerging consensus about the threat that the Big Tech companies pose to democracy” whereas “there is little agreement about how to respond”. To face these concerns, many critics demanded Internet platforms to assume greater responsability on the content they disclose, but only pressuring these platforms to act according to public interest is not a long-term solution [18]. Therefore, they brought up the suggestion of finding a technical solution, a so-called Middleware which is a “software that rides on top of an existing platform and can modify the presentation of underlying data”. Such a software should be added to current technology platforms’ services, and should “allow users to choose how information is curated and filtered for them”. Our technical solution goes in this direction: creating a system that mediates the interaction of the users with the digital world, by offering a personalized exoskeleton.

### 3.1. A Technical Proposal for Empowering the User and Limiting Producers' Autonomy.

In the absence of a satisfying regulation of autonomous systems, the power and the burden to preserve the users' rights remain in the hands of their producers. Hence, it seems necessary to raise the level of human-machine interaction, on the one hand, by empowering the user when interacts with the digital world, and on the other hand, by limiting producer's autonomy.

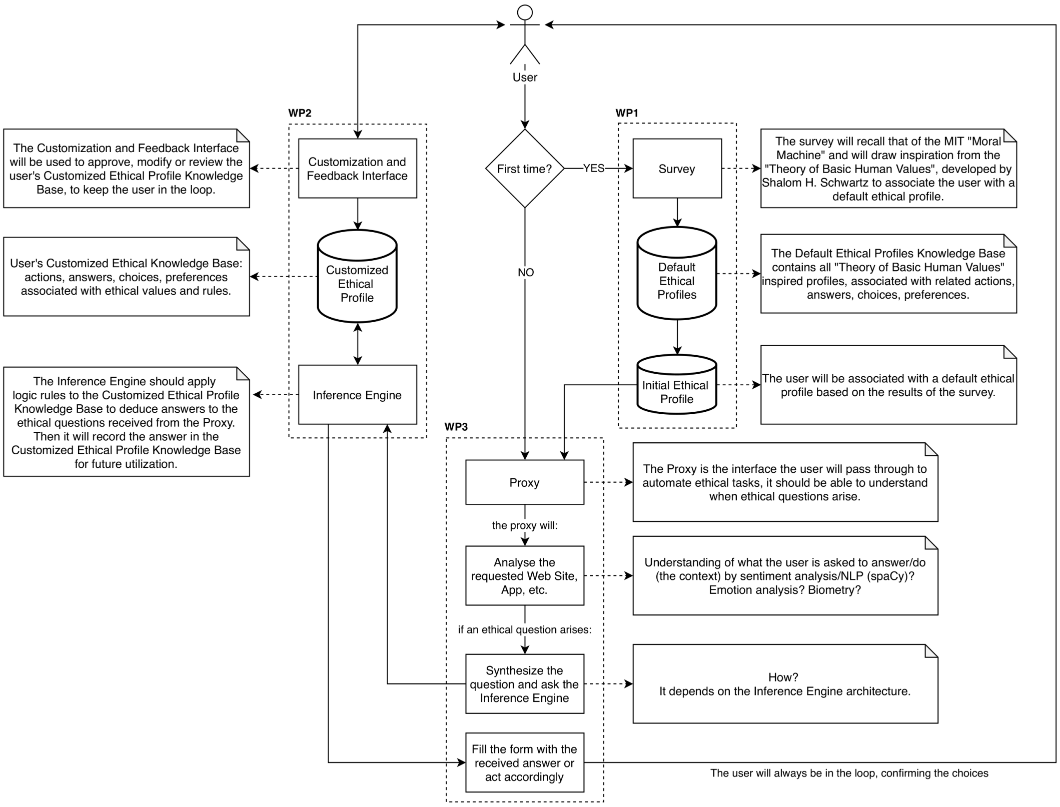
In this direction, the multidisciplinary EXOSOUL project[9] [19] aims to empower humans with an automatically generated exoskeleton, i.e. a software shield that protects them and their personal data through the mediation of all interactions with the digital world that would result in unacceptable or morally wrong behaviors according to their ethical and privacy preferences. The exoskeleton, composed by active data and ethical actuator, on one side governs the creation, destruction and sharing of personal data according to the owner ethical preferences, on the other side intercepts the interactions between the autonomous system and the user to prevent behaviours not acceptable according to the user's ethical profile (see Fig. 2). Therefore, such system relies on the ethical profiling of a user, which reflects her general moral preferences that are used to predict user's digital behaviors and to interact with the digital world according to this profile [20]. This is a strong point in user's protection: indeed, the exoskeleton operates according to individual preferences previously established, and it is less subject to the context in which it is deployed, as it is the case for many autonomous systems.

The adoption of an exoskeleton from citizen will turn into reality a negotiation between users and the digital world: indeed, the exoskeleton brings the individual preferences of the user and operates accordingly, by reversing the actual paradigm of passively accepting the way autonomous systems work. As suggested in [18, 19], the diffusion and adoption of exoskeletons or mediator software will create new opportunities for existing and new companies in the field of societal-friendly applications. This will create new actors in the digital economy sphere thus balancing the power of autonomous systems' producers.

The non-consideration of end-users in the AI Act has been highlighted by [17], for which their role of "subject of rights [. . . ] has been obscured and their human dignity neglected". A contribution to the current role of end-users could be provided by the deployment of exoskeletons, whose purpose to preserve human dignity is pursued by protecting individual preferences and their choices.

The ultimate goal of EXOSOUL is to restore a balance of power between users and entities in the digital world. Indeed, a wide adoption of exoskeletons from citizens will eventually force big players (such as Android, Apple, and automotive OEMs) to change the way they manage control policies, users' data, and ethics [19]. As already suggested in the following section, if user are empowered autonomous system producers will have to offer a wider number of choices and more customized preferences.

[9] The project participants' expertise cover multiple scientific areas: computer science, philosophy, psychology, sociology and jurists.


User
WP2
WP1
WP3
First time?
YES
NO
Survey
Default Ethical Profiles
Initial Ethical Profile
Customization and Feedback Interface
Customized Ethical Profile
Inference Engine
Proxy
the proxy will:
Analyse the requested Web Site, App, etc.
if an ethical question arises:
Synthesize the question and ask the Inference Engine
Fill the form with the received answer or act accordingly

The Customization and Feedback Interface will be used to approve, modify or review the user's Customized Ethical Profile Knowledge Base, to keep the user in the loop.

User's Customized Ethical Knowledge Base: actions, answers, choices, preferences associated with ethical values and rules.

The Inference Engine should apply logic rules to the Customized Ethical Profile Knowledge Base to deduce answers to the ethical questions received from the Proxy. Then it will record the answer in the Customized Ethical Profile Knowledge Base for future utilization.

The survey will recall that of the MIT "Moral Machine" and will draw inspiration from the "Theory of Basic Human Values", developed by Shalom H. Schwartz to associate the user with a default ethical profile.

The Default Ethical Profiles Knowledge Base contains all "Theory of Basic Human Values" inspired profiles, associated with related actions, answers, choices, preferences.

The user will be associated with a default ethical profile based on the results of the survey.

The Proxy is the interface the user will pass through to automate ethical tasks, it should be able to understand when ethical questions arise.

Understanding of what the user is asked to answer/do (the context) by sentiment analysis/NLP (spaCy)? Emotion analysis? Biometry?

How?
It depends on the Inference Engine architecture.

The user will always be in the loop, confirming the choices

**Figure 2:** EXOSOUL Ethical Engine Scheme.

## 3.2. Improving Human-machine Interaction: a Model of Moral Agreement.

In order to guarantee such an augmented interaction, a model of *moral agreement* is proposed, between machine and the users. Following this model, AI systems as far as individual rights are concerned, could leave to the users the choice of what they assume as fair, reasonable, satisfactory, in the aim of making autonomous systems flexible and adaptable to different individual values systems.

This solution is expected to reduce the risk that producers influence the machine's ethical ecosystem and, at the same time, to ensure a wide space to individual values systems. On the grounds of interests, preferences, values selected by the user, the AI system should offer acceptable and tailored solutions. By this way, the same system gains a higher level of adaptability to different, specific needs (and to different individual values systems).

From the point of view of the user, this means to have the chance of choosing among a wider and more customized range of preferences, but, at the same time, to accept to release some levels of privacy, since the precondition is the digital modeling of personal data (ethical profiling) although through a secure personalized software.

From the point of view of the producer, the model requests to open part of the decision interface to users through a simplification of the selection process and enlargement of choices, but, at the same time, it could reduce some risks (for ex., risk of discrimination) and enhance the user's trust in the system.

### 3.3. Juridical Grounds: Informed Consent as Pre-condition for the Moral Agreement's Validity.

From a juridical perspective, the proposed model of moral agreement highlights the theoretical category of contract and reiterates the model of the express and informed consent, also adopted by GDPR and traditionally considered an effective tool to guarantee self-determination and to protect individual rights.

Express and informed consent are very close conceptual categories, but not exactly the same, the first (express consent) being a consent pertaining specifically to the activity to which the consent is given, whereas the second (informed consent) requires a substantial understanding of the context in substantial absence of control by others. Informed consent has an ethical dimension, as it facilitates the transfer of information between two parties, allowing them "to become aware of the potential risks that may arise if they consent to a procedure or determine whether consenting to a procedure may conflict with their values or preferences" [21]. Informed consent would also have "a kind of symbolic value for parties, because it acknowledges them as decision makers and recognises their personhood" [21].

However, in the course of time the model of consent has showed a number of limits, with particular reference to:

- explainability: a free and specific consent is based on the knowledge and understanding of the context in which the same consent is done. This means that it should be possible to explain the internal mechanisms of a deep learning system in human terms. However, this exigence is limited by several factors, as, among others, the companies' reluctance to reveal their own internal working, or the extreme complexity of the same system (or the black-box phenomenon: "a machine learning algorithm may be so complex that not even the creators understand how it works) [22];
- transparency: the choice cannot be considered valid, if the user does not know the way of functioning of the algorithm[10]. Similarly, an overload of information can make the "informed consent" useless. Consent is no longer effective as it once was as mechanism of control, in case of excessive multiplication of choices;
- effectiveness: having a wide range of choice does not mean to express a specific consent for every moral preference. Express consent is not necessarily informed consent, as it could merely be a more complicated process. This implies to rethink the model of continual consent.

In sum, the problem of the informed consent lies in its fundamental assumption, that "individuals can understand all facts relevant to true choice at the moment of pair-wise contracting between individuals and data gatherers" [23]. This limit of the model of consent has been

[10] See C. Cass., ord. 25.05.2021, n. 14381, available at http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20210525/snciv@s10@a2021@n14381@tO.clean.pdf.

clearly showed during the last years in the GDPR implementation, and the experience of data protection can be easily translated to the discussion on AI systems.

Considering the above, a number of Authors proposed alternative solutions, such, for example, the adoption of a stringent rule-based approach to permissible and prohibited conducts [21], a 'soft governance' ethical regulation (not necessarily as an alternative, but as a complement of the first proposal), the growth of representativeness and diversification within AI development teams, the involvement of stakeholders in designing and building AI systems. As a different option, some scholars point out that "consent cannot be confused with choice" and must be defined "by its moral core", which includes account knowledge, voluntariness, and fairness. None of these proposals is taken into account, in the AI Act [24].

Being aware about these limits does not imply the refuse of the proposed model, but rather the necessity of rethinking informed consent as the unique and most effective tool to guarantee the protection of individual rights [21, 25, 26].

In any case, the paradigm of the contract – as a guarantee of voluntariness – needs to be integrated with the paradigm of responsibility, this last in its twofold dimension, of liability and accountability.

## 4. Conclusion

The AI Act is a big step that Europe has put forward in the AI regulation arena. In this paper we focus on its adequacy to protect individual rights and propose a different approach that have juridical and technical implications. The overarching principle that inspires us is that of human dignity: "the principle of human dignity, understood as the recognition of the inherent human state of being worthy of respect, must not be violated by 'autonomous' technologies" as stated by the European Group on Ethics in Science and New Technologies in [27]. Our approach to satisfy that principle is to guarantee an *even* interaction among system and user that may eventually result on the settlement of a moral agreement steered by the user. This is possible if the user during digital interactions can choose how to protect her dignity by means of alternative software tools, as suggested in [18]. In our proposal this role is played by the exoskeleton. Many steps forward have been done in the EXOSOUL project but many more are yet to come, for which a big multidisciplinary effort is demanded within the project's scientific community.

## References

[1] M. Ebers, Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act, The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics (2021).

[2] F. Caroccia, Ancora su responsabilità civile e uso delle intelligenze artificiali., Contratto e Impresa (2022).

[3] Artificial Intelligence Act. "Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts", EUR-Lex-

52021PC0206 (2021). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR:e0649735-a372-11eb-9585-01aa75ed71a1.

[4] G. Comandé, Intelligenza artificiale e responsabilità tra «liability» e «accountability». Il carattere trasformativo dell'IA e il problema della responsabilità, Analisi Giuridica dell'Economia 18 (2019) 169–188. Società editrice il Mulino.

[5] U. Salanitro, Intelligenza artificiale e responsabilità: la strategia della Commissione Europea, Rivista di diritto civile 66 (2020) 1246–1276.

[6] F. Doshi-Velez, M. Kortz, R. Budish, C. Bavitz, S. Gershman, D. O'Brien, K. Scott, S. Schieber, J. Waldo, D. Weinberger, et al., Accountability of AI under the law: The role of explanation, arXiv preprint arXiv:1711.01134 (2017).

[7] M. Veale, F. Z. Borgesius, Demystifying the draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach, Computer Law Review International 22 (2021) 97–112.

[8] M. Ebers, V. R. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, The european commission's proposal for an artificial intelligence act—a critical assessment by members of the robotics and ai law society (rails), J 4 (2021) 589–603.

[9] F. Ufert, Ai regulation through the lens of fundamental rights: How well does the gdpr address the challenges posed by ai?, European Papers-A Journal on Law and Integration 2020 (2020) 1087–1097.

[10] A. BERTOLINI, et al., Artificial intelligence and civil liability (2020).

[11] N. A. Smuha, E. Ahmed-Rengers, A. Harkens, W. Li, J. MacLaren, R. Piselli, K. Yeung, How the EU can achieve legally trustworthy AI: A response to the European Commission's proposal for an Artificial Intelligence Act, Available at SSRN (2021).

[12] N. A. Smuha, Beyond the individual: governing AI's societal harm, Internet Policy Review 10 (2021).

[13] R. M. Vasse'i, The ethical guidelines for trustworthy AI–A procrastination of effective law enforcement, Computer Law Review International 20 (2019) 129–136.

[14] L. Floridi, Translating principles into practices of digital ethics: Five risks of being unethical, in: Ethics, Governance, and Policies in Artificial Intelligence, Springer, 2021, pp. 81–90.

[15] T. Hagendorff, The ethics of ai ethics: An evaluation of guidelines, Minds and Machines 30 (2020) 99–120.

[16] R. Calo, Artificial intelligence policy: a primer and roadmap, UCDL Rev. 51 (2017) 399.

[17] L. Edwards, Regulating AI in Europe: four problems and four solutions., 2022. URL: https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/.

[18] F. Fukuyama, B. Richman, A. Goel, How to save democracy from technology: ending big tech's information monopoly, Foreign Aff. 100 (2021) 98.

[19] M. Autili, D. Di Ruscio, P. Inverardi, P. Pelliccione, M. Tivoli, A software exoskeleton to protect and support citizen's ethics and privacy in the digital world, IEEE Access 7 (2019) 62011–62021.

[20] P. Migliarini, G. L. Scoccia, M. Autili, P. Inverardi, On the elicitation of privacy and ethics preferences of mobile users, in: Proceedings of the IEEE/ACM 7th International Conference on Mobile Software Engineering and Systems, 2020, pp. 132–136.

[21] A. J. Andreotta, N. Kirkham, M. Rizzi, AI, big data, and the future of consent, Ai & Society (2021) 1–14.

[22] J. Burrell, How the machine ‘thinks’: Understanding opacity in machine learning algorithms, Big Data & Society 3 (2016) 2053951715622512.

[23] H. Nissenbaum, A contextual approach to privacy online, Daedalus 140 (2011) 32–48.

[24] E. Edenberg, M. L. Jones, Troubleshooting ai and consent (2020).

[25] S. C. Robinson, Trust, transparency, and openness: How inclusion of cultural values shapes nordic national public policy strategies for artificial intelligence (ai), Technology in Society 63 (2020) 101421.

[26] G. K. Y. CHAN, M. YIP, Ai, data and private law: The theory-practice interface (2021).

[27] E. G. on Ethics in Science, N. Technologies, et al., Statement on artificial intelligence, robotics and’autonomous’ systems: Brussels, 9 March 2018., EU: European Union, 2018.