Regulating Advanced Technologies

Policy Papers of the Jean Monnet Centre of Excellence on the Regulation of Robotics and AI – EURA

Jean Monnet Centre of Excellence

Co-funded by the Erasmus+ Programme of the European Union

Table of Contents

Jean Monnet Centre of Excellence

Co-funded by the Erasmus+ Programme of the European Union

Authors: *A. Bertolini* §§ 2.1, 2.5, 3.1, 3.4, 4.1, 4.6, 4.7; *R. Carli* §§ 2.2, 2.3, 2.4; *R. Limongelli* §§ 4.2, 4.3, 4.4, 4.5; *L. Sposini* §§ 3.2, 3.3, 3.4.

1. The Eura Policy Papers

The policy papers here collected are the purport of the work carried out by EURA and its teams during the entire project duration (August 2018-today), and rest upon the analysis carried out over a number of events and debates, including previous editions of the yearly EURA Conference, and seminars, all of which may still be watched on our website (https://www.eura.santannapisa.it/) and social media, in particular the EURA YouTube channel[1].

Indeed, one of the focal points of our Jean Monnet Centre of Excellence (CoE) is to establish a constant dialogue with policy-makers, identifying topics of relevance for societal debate, and selecting trends and issues relevant for businesses and investors.

Our members participate in various entities for the support of policy building in the area of robotics and embedment of ethical standards in AI system.

In order to convey to legislative and governmental entities the outcome of its research and activities, EURA released a number of opinions and policy-papers, providing early identification of relevant issues, assessment, recommendations, participating in many debates leading to the adoption of regulation, advancing proposals for actions to be taken.

EURA as an entity, as well as its fellows in their individual capacity, have participated in the policy debates on Artificial Intelligence, in particular about the AI Act, with a focus on prohibited practices and user deception, civil liability, risk-management and insurance, product safety, industrial and social robotics applications and platforms regulation.

[1] https://www.youtube.com/@eura-jeanmonnetcentreofexc3678

The papers here presented constitute an abridged, updated, and systematized version of some of the many contributions, also presented to EU and international institutions over the years, produced with the help of the Ph.D. students collaborating with the Centre, as indicated in the relevant sections:

The policy paper on "*Manipulation through AI systems*" was co-authored by **Rachele Carli** (§§2.2, 2.3 and 2.4) and Andrea Bertolini (§§2.1 and 2.5) and builds primarily upon the debate and articles published after the 2019 EURA Conference on "Human Robot Interaction between Trust and Deception", as well as the 2019 EURA Workshop "Europe Regulates Robotics", providing an early discussion and assessment of the AI Act[2], also with a focus on prohibited practices.

The policy paper on "*Digital Platforms and Liability*" was co-authored by **Ludovica Sposini** (§§3.2, 3.3 and 3.4) and Andrea Bertolini (§§3.1 and 3.4) and primarily builds upon the detailed study commissioned by the Panel for the Future of Science and Technology (STOA), "Liability of Online Platforms" of 2021[3], authored by Andrea Bertolini, Francesca Episcopo, and Nicoleta Angela Cherciu.

The study reviews the main legal/regulatory challenges associated with the operation of online platforms, the incentives for online platforms, their users and third parties, to detect and remove illegal/harmful and dangerous material, content and/or products; maps and critically assesses the whole range of online platforms liabilities, taking hard and soft law,

---

[2] European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts.
COM(2021) 206 final. Brussels, European Commission.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

[3] Bertolini, A., F. Episcopo and N. Cherciu (2021). Liability of Online Platforms. Brussels, European Parliament. The full study may be freely downloaded from:
https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)656318.

self-regulation, as well as national legislation into consideration; drafts policy options for an efficient EU liability regime.

The policy paper on "*Product Liability*" was co-authored by **Rocco Limongelli** (§§4.2, 4.3, 4.4 and 4.5) and Andrea Bertolini (§§4.1, 4.6 and 4.7) and primarily builds upon the detailed study commissioned by the Policy Department C at the request of the Committee on Legal Affairs, "Artificial Intelligence and Civil Liability"[4] of 2020, authored by Andrea Bertolini with the support of Francesca Episcopo, and Nicoleta Angela Cherciu. The study analyses the notion of AI-technologies and the applicable legal framework for civil liability. It demonstrates how technology regulation should be technology-specific, and presents a Risk Management Approach, where the party who is best capable of controlling and managing a technology-related risk is held strictly liable, as a single entry point for litigation. It then applies such approach to four case-studies, to elaborate recommendations.

Given the recent proposals for an AI Liability Directive[5] and on liability for defective products[6], and ongoing consultation initiated by the European Commission, the paper will be updated, taking into account the debate carried out in the 3rd EURA 2022 Conference "The Gift of

[4] Bertolini, A. (2020). Artificial Intelligence and Civil Liability. Bruxelles, European Parliament - Committee on Legal Affairs: 1-132. The full study may be freely downloaded from: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf.

[5] European Commission (2022). Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM(2022) 496 final. Brussels, European Commission. https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf.

[6] European Commission (2022). Proposal for a Directive of the European Parliament and of the Council on liability for defective products. COM(2022) 495 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0495&from=EN.

the Evil D-AI-ty. Regulating Data and AI in Europe", where a panel is going to address said matter. The updated version will then be submitted to the open consultation and distributed online via the CoE website.

2. Manipulation through AI systems

2.1 Introduction

AI based systems[7] are becoming more and more pervasive, with the prospect – more or less futuristic – of being included in many support, care, and entertainment activities directly involving human beings.

For this reason, research is focusing on making them accepted by end users, engendering trust and familiarity with these applications. The very expedients used to achieve this goal, however, can be generators of manipulative dynamics, that can expose individuals to danger, from a physical, economic, and – increasingly – psychological point of view.

The analysis presented here aims to investigate this phenomenon, starting with an analysis of the features implemented in order to facilitate the interaction (Section 2.2), and presenting a number of concrete cases – to make it easier to fully understand the possible implications (Section 2.3). This is essential in order to lay the foundations from which to examine the recent AI Act, highlighting its merits and criticalities (Section 2.3). Finally, recommendations will be made regarding the lines to be followed at a legal and regulatory level (Section 2.4), in order to resolve the problematic aspects of the current approach and ensure a European development of new technologies, which prioritises the protection of users' integrity and fundamental rights.

[7] High-Level Expert Group on Artificial Intelligence (2019). A definition of AI: main capabilities and disciplines. Brussels, European Commission. 1 ss., European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM/2021/206 final. Brussels, European Commission. 1 ss.

2.2 New technologies and appearance

From the famous Imitation Game onward, AI has been conceived and programmed through the logic of appearance[8].

What developers try to achieve by designing an artificial intelligence device – embodied or not – is the ability for the application to emulate certain human cognitive, relational, or emotional characteristics. The most common examples include the emulation of the people's intellectual or conversational abilities, empathic response, deep understanding – as we could expect from a long-time friend –, affection, detailed attention[9]. All these elements are functional to make a person feel comfortable using the application, but also provide her with an experience similar to that they would have with a human counterpart[10].

This can provide numerous technical advantages. First of all, the individual is more inclined to make prolonged and repeated use of the system. This allows the latter to acquire more data, thus increasing its operational sophistication[11]. Secondly, it makes up for the lack of human professional in some settings, such as the care of frail individuals, partially tied on an increasingly aging population[12]. To their very functioning human users may feel comfortable around such applications and

---

[8] Turing, A. (1950). "Computing Machinery and Intelligence." Mind **49**: 433-460. 1 ss. In his famous work, Alan Turing proposed an experiment aimed at demonstrating the ability of a computer to induce a person, placed in another room, to believe that they were conversing in writing form with a human peer and not with a machine. The computer capable of passing this test – also known as "the Turing Test" – would have proved not so much to be intelligent, as to know how to emulate in a sufficiently sophisticated way the conversational skills of a human being.

[9] Epley, N., A. Waytz and J. T. Cacioppo (2007). "On seeing human: a three-factor theory of anthropomorphism." Psychological review **114**(4): 864. 864 ss.

[10] Walter, W. G. (1950). "An imitation of life." Scientific american **182**(5): 42-45. 42-45

[11] Hamacher, A., N. Bianchi-Berthouze, A. G. Pipe and K. Eder (2016). Believing in BERT: Using expressive communication to enhance trust and counteract operational error in physical Human-robot interaction. 2016 25th IEEE international symposium on robot and human interactive communication (RO-MAN), IEEE. 493-500

[12] Niemelä, M. and H. Melkas (2019). Robots as social and physical assistants in elderly care. Human-centered digitalization and services, Springer**:** 177-197. 177-197

considered, as if they were being really cared for, which, however, they are not[13].

However, these dynamics can present several side-effects[14]. The rhetoric and design around new technologies is such as to target the human cognitive and psychological dimension, so as to elicit empathic and emotional responses, in spite of the individual level of rationality or awareness about the artificial mechanism behind a certain action, sentence, expression produced by the system.

Studies of cognitivism and neuroscience specifically establish which elements induce a given emotional reaction in the human beings involved[15], and those elements are then taken into account to design such mechanisms, both in their external appearance and functioning.

This is particularly relevant in the case of those applications or devices which are meant to interact with humans by emulating the possession of social[16] and cultural competences[17]. Some examples could be chatbots, robot companions and all those AI systems that are designed to perform roles of entertainment, recreation, assistance, care, or companionship.

---

13 Bertolini, A. and S. Arian (2020). Do robots care? Towards an Anthropocentric Framework in the Caring of Frail Individuals Through Assistive Technology. Aging between Participation and Simulation. Ethical Dimensions of Socially Assistive Technologies in Elderly Care. J. Haltaufderheide, J. Hovemann and J. Vollmann. Berlin, GE, De Gruyter**:** 35-52. 35-52

14 Sharkey, A. and N. Sharkey (2021). "We need to talk about deception in social robotics!" Ethics and Information Technology **23**(3): 309-316. 309-316

15 Natale, S. (2021). Deceitful Media. Artificial Intelligence and Social Life after the Turing Test. New York, Oxford University Press. 140 ss.

16 Breazeal, C., K. Dautenhahn and T. Kanda (2016). "Social robotics." Springer handbook of robotics: 1935-1972.

17 Riva, G. and E. Riva (2019). "CARESSES: The World's First Culturally Sensitive Robots for Elderly Care." Cyberpsychology, Behavior, and Social Networking **22**(6): 430-430.

2.3 New technologies and (potentially) inherent manipulation

With regards to software agents for entertainment and company, a classic prototype is represented by chatbots created to interact continuously and intimately with the user[18]. They are developed with the intent to imitate a wide range of human-to-human relationships, so as to show apparent interest, to give and to require attention, to induce the individual to engage ever more frequently with them. Before starting the very first interaction, people can choose the personality, character, chatting style and role that the chatbot has to emulate, creating a dynamic that simulates an interpersonal relationship, shaped on users' own will. Despite most applications of this kind being still rudimentary, those very characteristics are that retain users[19].

As a result of the psychological dependence that is likely to occur, the person is also induced to pay subscriptions in order to have access to features that make the dialogue more intimate and similar to what you would have with a human being.

A similar way to ensure users' satisfaction is used by home assistant robots[20]. In this case, they are endowed with a body, even if extremely existential in its physicality. The central aspect is, in this case, the voice, which must have an intonation, a cadence, and a volume such as to instil confidence, trust, and calm in the listener[21]. Here, the ability to increase use and interaction are essential to create a profiling of the person

---

[18] A possible example could be Replika, https://replika.ai/

[19] Hakim, F. Z. M., L. M. Indrayani and R. M. Amalia (2019). A dialogic analysis of compliment strategies employed by replika chatbot. Third International Conference of Arts, Language and Culture (ICALC 2018), Atlantis Press. 266-271

[20] As a possible example, among others, consider Alexa.

[21] Chattaraman, V., W.-S. Kwon, J. E. Gilbert and K. Ross (2019). "Should AI-Based, conversational digital assistants employ social-or task-oriented interaction style? A task-competency and reciprocity perspective for older adults." Computers in Human Behavior **90**: 315-330. 315-330

involved, in order to adapt the purchase recommendations to their tastes and personality[22].

To do this more effectively, the device simulates the ability to remember and understand the needs of its interlocutor, thus creating a friendly dynamic that leads to an increase in purchases and the delegation of daily decisions to the machine[23]. In this way, these devices may also interfere with the range of information that actually reaches the user – which is filtered *ex ante* by the device on the basis of the profiling results. Thus, choices, intention, tastes, and even actions could be influenced and manipulated. Once again, even the economic sphere must be considered, insofar as such devices can induce compulsive expenditure or, anyway, an increase in consumption based on "induced", more than concrete, needs.

The implications become even more articulated if we consider machines in which pleasant physical appearance[24], gazes, and movements can be used as instruments of interaction and elicitation of affective and emotional bonding[25].

---

[22] Natale, S. (2020). "To believe in Siri: A critical analysis of AI voice assistants." 47

[23] Chattaraman, V., W.-S. Kwon, J. E. Gilbert and K. Ross (2019). "Should AI-Based, conversational digital assistants employ social-or task-oriented interaction style? A task-competency and reciprocity perspective for older adults." Computers in Human Behavior **90**: 315-330. 315-330

[24] One of the most explicative examples is that of Jibo, a social robot developed by MIT in Boston, which consists of a base and a big round head including a screen on which luminous images appear, to give animation to the robot and through which it shares with the human being forms of apparent emotional interiority – affection, empathy, joy, etc.

For a deeper analysis, see: Van Camp, J. (2017). "Review: Jibo social robot." Wired **11**: 17. 11-17

[25] Breazeal, C. (2014). JIBO, The world's first social robot for the home [Internet]. Indiegogo. 2014. 40 ss.

In the long run, it has been proven that these devices cannot satisfy users' expectations, due to their evident technical shortcomings[26]. Nevertheless, in the short term it was noticed that people had been led to consider them as living creatures, like pets, and sometimes as real companions to whom to confide secrets and very sensitive data, ignoring the systems by which it recorded and exploited such data for different purposes.

It follows that, despite the unbridgeable distance between the clear artificial nature of AI systems and the subjective appearance they are able to create, new technologies are able to enter the deepest layers of our daily lives and to potentially alter our perception of reality, attitude, and emotions.

For these reasons, special cautions are needed, to at least mitigate the manipulative outcome of human-AI interaction.

2.4 The current legal framework

On April 21st 2021, the European Commission published the AI Act[27], which is a proposal for a uniform regulation of AI systems at a European level. It represents the first attempt to structure a law-based approach to the development, the placement on the market, and the use of AI applications and devices, so as to comply with the fundamental rights framework and the constitutional principles of the Member States.

With regard to the scope of this analysis, Article 5, com.1, letter (a) and (b) – addressing the so called "prohibited practices" – is particularly

---

[26] Taking as an example the above-mentioned robot Jibo (see 18), it was advertised as a "new best friend", as a device able to "share common memories" with the users, to get to "know" them better than anyone else. However, the first edition of the machine has proven to be a market failure, not being able to meet users' expectations. To deepen the theme, see: It Hoffman, G. (2019). "Anki, jibo, and kuri: What we can learn from social robots that didn't make it." IEEE Spectrum. 25-34

[27] European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM/2021/206 final. Brussels, European Commission. 1 ss.

relevant. It was affected by one of the most recent amendments to the original text of the document which, however, has not changed its salient features and problematic profiles.

The article aims to prevent the commercialisation and use of AI systems capable of manipulating users, by inducing them to make decisions that they would not have made otherwise. In doing so, it clearly highlights the value choices underlying the regulatory proposal, focused on a human-centric development of new technologies which takes individuals' integrity as a priority over scientific innovation.

In particular, letter (a) deals with "subliminal techniques" which could modify people's behaviour so as to be "reasonably likely" to cause physical or psychological harm[28]. The discipline here suggested undoubtedly has the merit of having brought the attention of legislators – and of companies, as a consequence – to the theme of manipulation.

However, no definition is provided for the concept of "subliminal techniques", in order to differentiate it from other forms of legally admissible and potentially beneficial persuasion[29]. In this sense, on the one hand the article does not seem to add any new elements to provisions that already prohibited such dynamics, even if in different fields (i.e. advertising)[30]. On the other hand, it does not seem to be directly applicable to many of the technologies that are the subject of this

[28]Article 5:
1. The following artificial intelligence practices shall be prohibited:
(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness with the objective to or the effect to materially distorting a person's behaviour in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm
[29] Sax, M. (2021). Between empowerment and manipulation: The ethics and regulation of for-profit health apps, Kluwer Law International BV.
[30] Freire, F. C., T. F. Lombao and A. V. Bermúdez (2015). "Editorial policies of European public broadcasters for the use of new social media." Revista Brasileira de Políticas de Comunicação(6). 24-38

discussion. In fact, the above-mentioned cases involve software and devices for which the expressions used to advertise them, the sentences they are programmed to use, and the physical appearance play a fundamental role in users' final perception and in the development of emotional bonds. However, all these elements, as much as the artificial nature of the AI with which the interaction takes part, are perfectly known or made accessible to the human counterpart. Therefore, they may not be considered "hidden", or introduced with mechanisms that overcome human consciousness. That, however, does not diminish their potential of manipulating and ultimately affecting human users.

An additional problematic profile is the reference to the kind of harms to be considered. It is worthwhile to have made explicit the fact that these technologies can impact the human psychological dimension, disrupting the decision-making, volitional, and – to some extents even – perceptive processes. At the same time, the legal category of "psychological harms" is among the most debated, mainly because of the difficulty in proving it and in proving the causal link between the act and the damage, in a sufficiently objective way. Moreover, any negative consequence affecting individual psychological integrity – as much as manipulation – should be defined as phenomena, rather than single events, which can manifest their effects in the long run, thereby blurring the chain of causes.

Moreover, prohibiting those AI systems that have "the objective" of manipulating is undoubtedly essential, but at the same time it covers a limited number of cases. Producers and programmers most of the time have no intent to harm or circumvent their customers. Conversely, here we tried to demonstrate that often those characteristics which are implemented for technical needs or to compress inefficiencies due to the current level of development of a technology, may be the same as those causing adverse effects. Assuming this means drastically reducing the applicability of the norm. The same result is reached if we consider technology which are not developed to, but are still "reasonably likely"

to generate manipulative dynamics. The level of deployment of AI systems and the longitudinal studies we have at the moment are by no means sufficient to give us a clear and objective idea of the level of risk that each class of applications may represent for different categories of users.

This latter aspect leads to the letter (b) of the same article, which focuses specifically on the theme of "vulnerability" – ascribed to specific groups in reason of their age, their disabilities, or their socio-economic situation – which cannot be exploited with both the intent, or the effect of manipulating the final user[31].

Considering the human-AI interaction dynamics explained above, despite the consequences said, manipulation substantially varying according to the setting, the circumstances of use, as well as characteristics of the users. In fact, vulnerability is rooted in the human condition[32], and may not be eradicated[33]. When a given form of vulnerability is tackled and eventually removed via a technological solution, another form might emerge, that might give rise to no lesser concerns than the previous[34]. Moreover, uncertainty resides with respect to the vulnerable group under Art. 5, com.1, letter (b).

---

[31] (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, disability or a specific social or economic situation, with the objective to or the effect of materially distorting the behaviour of a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm;

[32] Arendt, H. (1958). The Human Condition. Chicago, The University of Chicago Press. 375

[33] Coeckelbergh, M. (2013). Human being@ risk: Enhancement, technology, and the evaluation of vulnerability transformations, Springer. 209

[34] MacIntyre, A. (2009). Dependent Rational Animals. Why Human Beings Need the Virtues. London, Duckworth. 175

Moreover, the circumstance – common to both provisions – that the prohibition is made dependent upon the verification of material harmful consequences, only allows for *ex post* assessment of the producers and products once they are already distributed on the market and diffused. This leads both to ineffectiveness of the protection offered – which, by definition, will not prevent harming the users – and *ex ante* uncertainty for researchers and developers of technologies, who will not be able to determine with precision the admissibility of their product or service.

2.5 Recommendations

The AI Act is currently a proposal for regulation and, as such, still subject to reform. The lively debate in the scientific community on the matter will certainly produce recommendations that can be used for a deep reformulation of many articles and concepts, so as to remove the problematic aspects mentioned in this discussion. Certainly, the European Union's choice to opt for a regulation based on legal principles and legal instruments – avoiding the phenomenon of ethic washing[35] – is to be welcomed, for it will ensure the formulation of enforceable and binding solutions for the parties involved. This does not mean that all forecasts are acceptable or effective, as demonstrated above. However, the law has other resources to be applied to resolve doubtful cases, such as legal interpretation, moving from fundamental principles already referred to in other areas of the legal system[36]. Therefore:

1. Within such framework, it is advisable to favour a vertical, technology-specific approach to regulation, distinguishing between different kinds of AI-based applications[37].

---

[35] Wagner, B. (2018). Ethics as an escape from regulation. From "ethics-washing" to ethics-shopping? Being Profiled, Amsterdam University Press**:** 84-89. 84-89

[36] Sacco, R. (1991). "Legal formants. A Dynamic Approach to Comparative Law (Installment I of II)." The American Journal of Comparative Law **39**(1): 1-34. 343-401

[37] A. Bertolini, Artificial Intelligence does not exist! Defying the technology-neutrality narrative, in the regulation of civil liability for advanced technologies. (forthcoming), in Europa e diritto privato, 2022.

2. Similarly, it could be advisable to delve deeper into the theme of manipulation, trying to trace lines to differentiate prohibited from those that should be permitted.
   Indeed, not all the cases described above (§2.2.1) ought to be deemed illicit *per se*, while still requiring ad-hoc regulation to sufficiently protect users.
3. Nudging mechanisms[38] could provide in many cases a preferable alternative. They consist of a modification to the choice architecture which leaves all the alternatives available to the individuals, with the end to benefit both the recipient and society[39]. Those practices would not be prohibited, since they do not engender coercion and do not induce actions that go beyond conscience and rationality.
4. Nevertheless, the problem arises of distinguishing what can actually be recognised as nudging and where the boundary between positive persuasion and manipulation in the perception of reality – and the actual basket of choices itself – must be established. This is particularly relevant in virtue of the fact that any legal solution, in order to be able to operate in concrete and to be effective with regard to its intended purpose, must be based on a clear and precise identification of the object to be regulated, of its specific characteristics, and of the similar phenomena from which it must be differentiated.
5. In parallel to this, the identification of specific obligations and duties in the design and programming processes may represent a good solution to solve the problem of lack of *ex ante* legal certainty.

[38] Thaler, R. H. and C. R. Sunstein (2021). Nudge, Yale University Press. 384-390
[39] Thaler, R. H. and C. R. Sustein (2008). Nudge: Improving Decisions about Health, Wealth, and Happiness. New Haven, Yale University Press. 365-373

This could both (i) foster research and development, ensuring that an AI system complying with these obligations cannot be deemed prohibited at a later date, (ii) provide safety and protection for users – not only in terms of the material safety of the product, but also in terms of mitigating possibly manipulative effects.

Bibliography

Arendt, H. (1958). The Human Condition. Chicago, The University of Chicago Press.

Bertolini, A. and S. Arian (2020). Do robots care? Towards an Anthropocentric Framework in the Caring of Frail Individuals Through Assistive Technology. Aging between Participation and Simulation. Ethical Dimensions of Socially Assistive Technologies in Elderly Care. J. Haltaufderheide, J. Hovemann and J. Vollmann. Berlin, GE, De Gruyter**:** 35-52.

Breazeal, C. (2014). JIBO, The world's first social robot for the home [Internet]. Indiegogo. 2014.

Breazeal, C., K. Dautenhahn and T. Kanda (2016). "Social robotics." Springer handbook of robotics: 1935-1972.

Chattaraman, V., W.-S. Kwon, J. E. Gilbert and K. Ross (2019). "Should AI-Based, conversational digital assistants employ social-or task-oriented interaction style? A task-competency and reciprocity perspective for older adults." Computers in Human Behavior **90**: 315-330.

Coeckelbergh, M. (2013). Human being@ risk: Enhancement, technology, and the evaluation of vulnerability transformations, Springer.

Epley, N., A. Waytz and J. T. Cacioppo (2007). "On seeing human: a three-factor theory of anthropomorphism." Psychological review **114**(4): 864.

European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending

certain union legislative acts. COM/2021/206 final. Brussels, European Commission.

Freire, F. C., T. F. Lombao and A. V. Bermúdez (2015). "Editorial policies of European public broadcasters for the use of new social media." Revista Brasileira de Políticas de Comunicação(6).

Hakim, F. Z. M., L. M. Indrayani and R. M. Amalia (2019). A dialogic analysis of compliment strategies employed by replika chatbot. Third International Conference of Arts, Language and Culture (ICALC 2018), Atlantis Press.

Hamacher, A., N. Bianchi-Berthouze, A. G. Pipe and K. Eder (2016). Believing in BERT: Using expressive communication to enhance trust and counteract operational error in physical Human-robot interaction. 2016 25th IEEE international symposium on robot and human interactive communication (RO-MAN), IEEE.

High-Level Expert Group on Artificial Intelligence (2019). A definition of AI: main capabilities and disciplines. Brussels, European Commission.

Hoffman, G. (2019). "Anki, jibo, and kuri: What we can learn from social robots that didn't make it." IEEE Spectrum.

MacIntyre, A. (2009). Dependent Rational Animals. Why Human Beings Need the Virtues. London, Duckworth.

Natale, S. (2020). "To believe in Siri: A critical analysis of AI voice assistants."

Natale, S. (2021). Deceitful Media. Artificial Intelligence and Social Life after the Turing Test. New York, Oxford University Press.

Niemelä, M. and H. Melkas (2019). Robots as social and physical assistants in elderly care. Human-centered digitalization and services, Springer**:** 177-197.

Riva, G. and E. Riva (2019). "CARESSES: The World's First Culturally Sensitive Robots for Elderly Care." Cyberpsychology, Behavior, and Social Networking **22**(6): 430-430.

Sacco, R. (1991). "Legal formants. A Dynamic Approach to Comparative Law (Installment I of II)." The American Journal of Comparative Law **39**(1): 1-34.

Sax, M. (2021). Between empowerment and manipulation: The ethics and regulation of for-profit health apps, Kluwer Law International BV.

Sharkey, A. and N. Sharkey (2021). "We need to talk about deception in social robotics!" Ethics and Information Technology **23**(3): 309-316.

Thaler, R. H. and C. R. Sunstein (2021). Nudge, Yale University Press.

Thaler, R. H. and C. R. Sustein (2008). Nudge: Improving Decisions about Health, Wealth, and Happiness. New Haven, Yale University Press.

Turing, A. (1950). "Computing Machinery and Intelligence." Mind **49**: 433-460.

Van Camp, J. (2017). "Review: Jibo social robot." Wired **11**: 17.

Wagner, B. (2018). Ethics as an escape from regulation. From "ethics-washing" to ethics-shopping? Being Profiled, Amsterdam University Press**:** 84-89.

Walter, W. G. (1950). "An imitation of life." Scientific american **182**(5): 42-45.

3. Digital Platforms and Liability

3.1 The issue

Digital platforms have assumed an increasingly central role in commercial as well as social relations. Indeed, they have brought about the birth of a new era of digitalisation, where a few large platforms hold enough economic power to influence the market itself. They act both as intermediaries between different groups of actors and as real economic agents offering different goods and services, thus creating a digital ecosystem that aspires to absorb all aspects of human life. It is clear, then, their position of dominance and the high concentration from which this 'new' business model suffers, characterised by the presence of these large players who set the conditions not only of access to their digital community, but also of permanence in it, including the mechanisms for managing and resolving any disputes that might arise within it.[40]

In modern society, in fact, it is well known that platforms now represent the main access point to an infinite amount of information, a circumstance which, on the one hand, favours pluralism of information and freedom of expression, on the other hand, poses several dangers for

[40] For the characteristics of the *platform economy,* see Seppälä, T., M. Halén, J. Juhanko, H. Korhonen, J. Mattila, P. Parviainen, J. Talvitie, H. Ailisto, K.-M. Hyytinen and J. Kääriäinen (2015). The Platform–History, Characteristics, and the Definition, The Research Institute of the Finnish Economy.; Wang, B. and X. Li (2017). "Big data, platform economy and market competition: a preliminary construction of plan-oriented market economy system in the Information Era." World Review of Political Economy **8**(2): 138-161.-161; Hoang, L., G. Blank and A. Quan-Haase (2020). "The winners and the losers of the platform economy: Who participates?" Information, Communication & Society **23**(5): 681-700.-700; Lafuente, E., Z. J. Ács and L. Szerb (2022). "Analysis of the digital platform economy around the world: A network DEA model for identifying policy priorities." Journal of Small Business Management: 1-45..

users including, in particular, the dissemination of illegal and/or harmful content.

Since platforms no longer play a role of mere digital intermediation but govern the entire digital ecosystem with an ever-increasing impact on the various aspects of both the social and commercial life of individuals, it becomes necessary to ask whether the current European legal framework is still adequate to guarantee effective protection of online users and their fundamental rights (such as the right to health, expression and information) with particular reference to the liability regime of platforms for illegal and harmful content disseminated by third parties through the provider itself.

To date, the legal framework is particularly complex and fragmented, given that platforms are held liable according to different 'types' of liability: on the one hand, the 'general' liability for harmful and/or illegal content posted and activities performed by platform users, and on the other hand, those specifically provided for by sectoral legislation such as, for instance, liability arising from infringement of intellectual property laws; product safety; protection of minors; hate speech and others.[41]

3.2 Major Challenges

The already fragmented legal framework is further complicated by the difficulties, given the heterogeneity and size of the providers, of circumscribing the phenomenon through the identification of a possible unitary definition of 'digital platform'.

[41] See Fabo, B., J. Karanovic and K. Dukova (2017). "In search of an adequate European policy response to the platform economy." Transfer: European Review of Labour and Research **23**(2): 163-175.-175; Busch, C. (2016). "The rise of the platform economy: a new challenge for EU consumer law?" Journal of European Consumer and Market Law **5**(1).; Cohen, J. E. (2017). "Law for the platform economy." UCDL Rev. **51**: 133..

In fact, the EU expressly recognised the impossibility and inappropriateness of constructing a clear-cut definition that would encompass all types of digital platforms.[42]

The most common approach to the phenomenon also used by the Commission is the economic one, according to which digital platforms are 'matchmarkers' that attract multiple consumers or groups of users and enable them to interact. It seems to follow from this definition that, in order to be able to speak of a digital platform, two elements must be present, namely they must be 'multisided', and they must 'facilitate interactions'. This then means that, according to the economic perspective, a digital platform consists of a 'digital service[s] that facilitate interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet at least in one direction'.[43]

However, this definition has obvious limitations, for at least two reasons. First, it excludes those online service providers operating as single-sided providers such as, for instance, media-services providers offering an on-demand streaming service of films or television series.[44] Such platforms, in fact, not only do not operate on both sides of the market, but also cannot be said to be mediators allowing different types of users to

[42] The term 'digital platform' itself takes on a different meaning depending on the type of sector being considered, as, for instance, science-engineers use the term to refer to a set of technologies or interfaces available to a broad base of users who build processes, applications, technologies and business models with it and on it, whereas social scientists and policy-makers understand it as those triangular digital structures that enable interactions between different groups of users, encompassing not only the entire structure itself and the entity that materially conducts such a service, but also the economic model adopted. Given the extreme diversity of platforms, then, it would be more desirable for the EU to adopt a case-by-case approach rather than construct a 'law of platforms. See Bertolini, A., F. Episcopo and N. Cherciu (2021). Liability of Online Platforms. Brussels, European Parliament 1-150.

[43] See OECD (2019). An introduction to Online Platforms., p. 20.

[44] See SWD(2016) 172 final, pp. 2-3.

interact with each other.[45] Secondly, considering digital platforms as agents enabling interaction between the various sides of the market would risk extending this definition also to Internet Service Providers (ISPs) who, instead, should be kept clearly separate.[46] These two categories of subjects, in fact, present profound differences between them because, ISPs merely offer the structure for accessing the Internet, whereas digital platforms, on the other hand, go much further because they not only offer the possibility of surfing online, but above all provide a series of services and products that aim at creating a true virtual community, in which the user - whether professional or consumer - is inevitably trapped.[47]

Notwithstanding the impossibility of formulating a definitive definition of a digital platform,[48] in any case, it remains useful to study and develop at least a functional definition that can help to find one way among the

---

[45] It should also not be forgotten that a platform may choose to adopt a different business strategy and thus not operate on both sides of the market. See Rochet, J.-C. and J. Tirole (2004). "Two-sided markets: An overview." Institut d'Economie Industrielle working paper.. According to Hagiu, A. and J. Wright (2015). "Multi-Sided Platforms." International Journal of Industrial Organization **43**: 162-174.-174 also consider the element of 'direct interactions between sellers and buyers or between two or more distinct sides' to be an essential feature of digital platforms.

[46] See Savin, A. (2018). "Regulating internet platforms in the EU - The emergence of the 'Level playing Field'." Computer Law & Security Review **34**(6): 1215-1231.-1231.

[47] BEREC ((2018). BEREC report on the impact of premium content on ECS markets and the effect of devices on the open use of the Internet., p. 24 ff.

[48] It should be pointed out that there have been numerous attempts in the literature to provide a definition of digital platforms, suffice it to mention Sun, R., S. Gregor and B. Keating (2016). "Information technology platforms: Definition and research directions." arXiv preprint arXiv:1606.01445;, Bacache-Beauvallet, M. and M. Bourreau (2020). Platforms. Handbook of Cultural Economics, Third Edition, Edward Elgar Publishing.; Sanchez-Cartas, J. M. and G. León (2021). "Multisided platforms and markets: A survey of the theoretical literature." Journal of Economic Surveys **35**(2): 452-487.-487; Asemani, M., F. Abdollahei and F. Jabbari (2019). Understanding IoT platforms: Towards a comprehensive definition and main characteristic description. 2019 5th International Conference on Web Research (ICWR), IEEE., 172-177; Baldwin, C. Y. and C. J. Woodard (2009). "The architecture of platforms: A unified view." Platforms, markets and innovation **32**: 19-44.-44.

numerous types of platforms, so as to better identify their duties and, above all, the applicable liability regime because, otherwise, one runs the risk of incurring either hyper-regulation (undesirable because it is a potential obstacle to technological development) or deregulation (undesirable because it would leave individuals entirely at the mercy of the power and dominant position of digital platforms).

It is clear that the impossibility of providing a unitary definition of these digital giants, as well as their extreme diversity, also gives rise to a difficulty in identifying the liability regime applicable to them.[49] As things stand, in fact, the legal framework applicable to them consists of a general liability regime for illegal and/or harmful content disseminated by third parties as set forth in Directive 2000/31/EC (ECD)[50] , further complementary liability regimes deriving from sectoral legislation[51] , as well as soft law documents and self-regulatory instruments such as codes of conduct.

[49] Depending on the type of service or activity they conduct, digital platforms are liable for primary liability, i.e. if they fail to fulfil an obligation directly attributable to them (think, for example, of the information and transparency obligations imposed on platforms vis-à-vis commercial users under Regulation (EU) 2019/1150). Similarly, there is also a secondary liability on the part of the platforms, to which they are subject whenever the third party, the first obligor, does not fulfil this obligation. In this hypothesis, then, the platforms are liable for the mere fact of being intermediaries through which the illegal and/or harmful content is disseminated online. See Riordan, J. (2020). "A Theoretical Taxonomy of Intermediary Liability."; Tereszkiewicz, P. (2018). "Digital platforms: regulation and liability in the EU law." European Review of Private Law **26**(6)..

[50] SeeEuropean Parliament and C. o. t. E. Union (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1–16..

[51] For an in-depth discussion of the different sectoral laws for particular platform liability scenarios, please refer to Bertolini, A., F. Episcopo and N. Cherciu (2021). Liability of Online Platforms. Brussels, European Parliament 1-150., pp. 34-69.

3.3 The current legal framework

At the European level, the general liability regime is primarily represented by the 'E-commerce Directive' (ECD), which constructs a system of gradation of (secondary) liability of intermediaries, so called 'Safe Harbor Regime', for illegal content disseminated by third parties online, although in any case it excludes the possibility for Member States to impose a general monitoring obligation on the content itself.[52] This system is based on the distinction between 'active' and 'passive' providers, in the belief that only where providers play an active role in the management of content can they be held liable for damages caused by the dissemination of such illegal content.[53]

Therefore, where the service provider's activity is *merely conduit*, it cannot be held liable for such information provided, however, that it does not give rise to the transmission and it does not select either the recipient of the transmission or the information transmitted.[54] *Caching providers*, on the other hand, are not liable as long as they do not modify the information; they comply with the conditions of access to the information as well as the widely recognised and used industry standards for updating the information; they do not interfere with the lawful use of technology widely recognised and used in the industry to obtain data on the use of the information; and, finally, they act 'promptly' to remove the stored

---

[52] Art. 15 ECD.

[53] On the distinction between 'active' and 'passive' intermediaries, let us refer to the considerations of the Court of Justice of the EU: Cases C-236/08 to C-328/08 Google France v Louis Vuitton EU:C:2010:159; Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, Case C-484/14, EU:C:2016:689.

[54] Article 12, par. 2, of ECD states that: 'The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission'. For a comment, see Johnson, A. and D. Castro ((2021). How Other Countries Have Dealt With Intermediary Liability, Information Technology and Innovation Foundation..

information or to disable access to it as soon as they become effectively aware that access to it has been disabled, that it has been removed from its original location, or if an administrative authority or court has ordered its removal or disabling of access to it.[55] On the other hand, the regime for *hosting providers* is more onerous because they are not held liable only if they are not aware of the unlawfulness of the information or activity and provided that, where they have become aware of it, they act 'expeditiously' to remove such content or to disable access to it.[56]

The European legislator, considering the liability regime outlined by the ECD to be obsolete with respect to the new digital services that have developed in recent years, decided to update this discipline with Regulation (EU) 2022/2065 ('Digital Service Act'), which aims to make the online environment a safe, predictable and reliable place through the imposition of a wide range of obligations that vary according to the size and impact of the digital service provided.[57]

---

[55] Art. 13, ECD. It has been observed that one of the most critical points of the ECD is precisely the lack of specification of what is meant by an 'expeditious reaction' to remove information. See Baistrocchi, P. A. (2002). "Liability of intermediary service providers in the EU Directive on Electronic Commerce." Santa Clara Computer & High Tech. LJ **19**: 111.; Bertolini, A., F. Episcopo and N. Cherciu (2021). Liability of Online Platforms. Brussels, European Parliament 1-150., p. 32.

[56] Art. 14, ECD. See Buiten, M. C., A. De Streel, Peitz and Martin (2020). "Rethinking liability rules for online hosting platforms." International Journal of Law and Information Technology **28**(2): 139-166.-166.

[57] See Parliament, E. ((2020). Digital Services Act: Improving the functioning of the Single Market. European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). TEXTS ADOPTED Brussels. andEuropean Parliament and C. o. t. E. Union (2022). 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, PE/30/2022/REV/1, OJ L 277, 27.10.2022, p. 1–102. Brussels . In literature, see, *ex multis*, Montagnani, M. L. (2019). "A New Liability Regime for Illegal Content in the Digital Single Market Strategy." Available at SSRN 3398160.; Frosio, G. F. (2017). "Reforming intermediary

This regulation essentially leaves the hypotheses of exemption from platform liability untouched, maintaining the tripartite structure between *mere conduit, caching* and *hosting providers*, but broadening the group of information service providers to which they apply.[58]

Due diligence obligations applicable to all intermediary service providers, including digital platforms, are then outlined, such as: designating a single point of contact to facilitate communication with the supervising authorities; a set of disclosure obligations, in particular on the terms and conditions of service; reporting obligations on the measures implemented to handle reports of illegal content and to resolve complaints;[59] provision of mechanisms for reporting illegal content[60] as well as the duty to promptly inform the competent authorities where such platforms become aware of information from which it is highly

liability in the platform economy: A European digital single market strategy." Nw. UL Rev. Online **112**: 18..

[58] It should be noted, however, that Member States are still prohibited from imposing general monitoring obligations on platforms under Article 8 of the DSA.

[59] Art. 15, DSA.

[60] These are the so-called 'notice and action' mechanisms referred to in Article 16: 'Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly and shall allow for the submission of notices exclusively by electronic means'. The legislator considers that such notifications 'shall be deemed to give rise to actual knowledge or awareness', with the consequence that the provider will no longer benefit from the exception of liability. As has been correctly noted, this requirement 'At scale, this will create very strong incentives for providers to simply remove any notified content and none of the safeguards provided in the DSA will have much effect in preventing this', see Cauffman, C. and C. Goanta (2021). "A New Order: The Digital Services Act and Consumer Protection." European Journal of Risk Regulation **12**(4): 758-774.-774; Chomanski, B. (2021). "The Missing Ingredient in the Case for Regulating Big Tech." Minds and Machines **31**(2): 257-275.-275; Wilman, F. (2020). The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US, Edward Elgar Publishing .

likely that a crime has been committed, is being committed or will be committed.[61]

In addition to these general obligations that apply across the board to all providers, there are further requirements that apply to very large platforms and search engines (i.e. with an average monthly number of active service recipients in the Union of no less than 45 million), which must, for instance provide to the public in an easily accessible and readable manner and at least annually reports on the moderation activities carried out during this period; carry out an analysis of systemic risks (among which are the dissemination of illicit content or in any case content that infringes fundamental rights; electoral processes; protection of minors) arising from both the design of the service and its use, with the consequent obligation to take appropriate measures to mitigate them; and, furthermore, participate in the drafting of codes of conduct as well as make algorithms available to the authorities.[62]

3.4 Recommendations

The economic and social power acquired by digital platforms in a very short period of time has brought with it risks and criticalities whose consideration can no longer be postponed if we really want to make the online environment a safe and reliable place that can ensure the protection of users' fundamental rights and freedoms.

The European legal framework on the subject sees the application not only of hard-law rules either harmonised at supranational level or adopted by individual Member States (with consequent fragmentation of

[61] Specific provisions on advertising and the protection of minors online, as well as in the case of platforms enabling consumers to conclude distance contracts with consumers, are also provided for in the Regulation.

[62] For a more in-depth analysis, please refer to Madiega, T. (2020). "Digital services act." European Parliamentary Research Service, PE.; Barczentewicz, M. (2021). "The Digital Services Act: Assessment and Recommendations." Available at SSRN 3874961..

the discipline), but also of soft-law instruments such as codes of conduct. Each of these rules has a different scope of application: some, they have transversal effectiveness because they are applicable to all digital platforms and others, on the other hand, are only applicable to certain specific types of platforms, specific infringements, or specific activities.[63]

Against this background, the following policy recommendations may be formulated:

1. In order then to avoid uncertainty about the liability regime applicable to these digital operators, it is necessary to establish a precise set of obligations on the basis of a 'technology-specific approach', i.e., tailored to the individual types of risks or injuries incurred as well as to the characteristics of the platforms involved.[64]
2. Given the global dimensions of the phenomenon, the different interests and rights that may come into play when surfing online through platforms, it is clear that it becomes essential to adopt a holistic approach, i.e., to consider the interconnection between the various legislations that cannot - and should not - be considered as stand-alone sectors.
3. For this, the European institutions should define the duties and responsibilities of platforms through precise and binding rules and, to do so, it seems advisable to maintain a 'baseline' regulatory regime supplemented by further sectoral regulations.

---

[63] Joanna Hornik and I. Villa (2017). "An Economic Analysis of Liability of Hosting Services: Uncertainty and Incentives Online." Bruges European Economic Research Papers **37**..

[64] This approach contrasts with the principle of 'technological neutrality' often used to assert regulation based on general definitions and clauses, so as to have the advantage of legislation that is adaptable to technological developments and does not need constant revision. On this point, see Koops, B.-J. (2006). "Should ICT Regulation be Technology-Neutral?" Cyberspace Law eJournal **9**., 77-108; Greenberg, B. A. (2015). "Rethinking technology neutrality." Minn. L. Rev. **100**: 1495..

According to this approach, it would be possible to impose a specific duty on the provider to act whenever it acquires evidence of the illegality of a content as well as to take measures to prevent the violation of the fundamental rights of other users. If, on the contrary, the platform fails to do so and does not achieve these objectives, it will have to be held liable for damages caused to the holder of the right or interest as well as to all those harmed by that content.

4. On the other hand, looking at the various sectoral legislations, it would be desirable to identify a strict and absolute liability system envisaged for large transaction platforms in the event of damage caused by defective or, in any case, harmful products and services offered on the platform itself by other users. In this hypothesis, in fact, the provider holds a position of control such as to allow the adoption of a solution similar to the one used by the courts in the United States, i.e. a form of strict and objective liability based on a risk management approach along the lines of what is already provided for at a European level with regard to the liability regime of importers and distributors of defective products pursuant to Article 3 of the Product Liability Directive.[65]

---

[65] Communities, C. o. t. E. (1985). Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, p. 29–33.Article 3(2) and (3) of which reads as follows: 'Without prejudice to the liability of the producer, any person who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business shall be deemed to be a producer within the meaning of this Directive and shall be liable as a producer.
3. Where the producer of the product cannot be identified, each supplier of the product shall be treated as its producer unless he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product. The same shall apply, in the case of an imported product, if this product does not indicate the identity of the importer referred to in paragraph 2, even if the name of the producer is indicated'. For a more detailed discussion of this approach, see Bertolini,

Bibliography

Asemani, M., F. Abdollahei and F. Jabbari (2019). Understanding IoT platforms: Towards a comprehensive definition and main characteristic description. 2019 5th International Conference on Web Research (ICWR), IEEE.

Bacache-Beauvallet, M. and M. Bourreau (2020). Platforms. Handbook of Cultural Economics, Third Edition, Edward Elgar Publishing.

Baistrocchi, P. A. (2002). "Liability of intermediary service providers in the EU Directive on Electronic Commerce." Santa Clara Computer & High Tech. LJ **19**: 111.

Baldwin, C. Y. and C. J. Woodard (2009). "The architecture of platforms: A unified view." Platforms, markets and innovation **32**: 19-44.

Barczentewicz, M. (2021). "The Digital Services Act: Assessment and Recommendations." Available at SSRN 3874961.

BEREC ((2018). BEREC report on the impact of premium content on ECS markets and the effect of devices on the open use of the Internet.

Bertolini, A., F. Episcopo and N. Cherciu (2021). Liability of Online Platforms. Brussels, European Parliament 1-150.

Buiten, M. C., A. De Streel, Peitz and Martin (2020). "Rethinking liability rules for online hosting platforms." International Journal of Law and Information Technology **28**(2): 139-166.

A., F. Episcopo and N. Cherciu (2021). Liability of Online Platforms. Brussels, European Parliament 1-150., p. 73; Palmerini, E. and A. Bertolini (2016). Liability and risk management in robotics. Digital revolution: challenges for contract law in practice, Nomos Verlagsgesellschaft mbH & Co. KG., 225-260.

Busch, C. (2016). "The rise of the platform economy: a new challenge for EU consumer law?" Journal of European Consumer and Market Law **5**(1).

Cauffman, C. and C. Goanta (2021). "A New Order: The Digital Services Act and Consumer Protection." European Journal of Risk Regulation **12**(4): 758-774.

Chomanski, B. (2021). "The Missing Ingredient in the Case for Regulating Big Tech." Minds and Machines **31**(2): 257-275.

Cohen, J. E. (2017). "Law for the platform economy." UCDL Rev. **51**: 133.

Communities, C. o. t. E. (1985). Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, p. 29–33.

European Parliament and C. o. t. E. Union (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1–16.

European Parliament and C. o. t. E. Union (2022). 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, PE/30/2022/REV/1, OJ L 277, 27.10.2022, p. 1–102. Brussels

Fabo, B., J. Karanovic and K. Dukova (2017). "In search of an adequate European policy response to the platform economy." Transfer: European Review of Labour and Research **23**(2): 163-175.

Frosio, G. F. (2017). "Reforming intermediary liability in the platform economy: A European digital single market strategy." Nw. UL Rev. Online **112**: 18.

Greenberg, B. A. (2015). "Rethinking technology neutrality." Minn. L. Rev. **100**: 1495.

Hagiu, A. and J. Wright (2015). "Multi-Sided Platforms." International Journal of Industrial Organization **43**: 162-174.

Hoang, L., G. Blank and A. Quan-Haase (2020). "The winners and the losers of the platform economy: Who participates?" Information, Communication & Society **23**(5): 681-700.

Joanna Hornik and I. Villa (2017). "An Economic Analysis of Liability of Hosting Services: Uncertainty and Incentives Online." Bruges European Economic Research Papers **37**.

Johnson, A. and D. Castro ((2021). How Other Countries Have Dealt With Intermediary Liability, Information Technology and Innovation Foundation.

Koops, B.-J. (2006). "Should ICT Regulation be Technology-Neutral?" Cyberspace Law eJournal **9**.

Lafuente, E., Z. J. Ács and L. Szerb (2022). "Analysis of the digital platform economy around the world: A network DEA model for identifying policy priorities." Journal of Small Business Management: 1-45.

Madiega, T. (2020). "Digital services act." European Parliamentary Research Service, PE.

Montagnani, M. L. (2019). "A New Liability Regime for Illegal Content in the Digital Single Market Strategy." Available at SSRN 3398160.

Palmerini, E. and A. Bertolini (2016). Liability and risk management in robotics. Digital revolution: challenges for contract law in practice, Nomos Verlagsgesellschaft mbH & Co. KG.

Parliament, E. ((2020). Digital Services Act: Improving the functioning of the Single Market. European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)). TEXTS ADOPTED Brussels.

Riordan, J. (2020). "A Theoretical Taxonomy of Intermediary Liability."

Rochet, J.-C. and J. Tirole (2004). "Two-sided markets: An overview." Institut d'Economie Industrielle working paper.

Sanchez-Cartas, J. M. and G. León (2021). "Multisided platforms and markets: A survey of the theoretical literature." Journal of Economic Surveys **35**(2): 452-487.

Savin, A. (2018). "Regulating internet platforms in the EU - The emergence of the 'Level playing Field'." Computer Law & Security Review **34**(6): 1215-1231.

Seppälä, T., M. Halén, J. Juhanko, H. Korhonen, J. Mattila, P. Parviainen, J. Talvitie, H. Ailisto, K.-M. Hyytinen and J. Kääriäinen (2015). The Platform–History, Characteristics, and the Definition, The Research Institute of the Finnish Economy.

Sun, R., S. Gregor and B. Keating (2016). "Information technology platforms: Definition and research directions." arXiv preprint arXiv:1606.01445;.

Tereszkiewicz, P. (2018). "Digital platforms: regulation and liability in the EU law." European Review of Private Law **26**(6).

Wang, B. and X. Li (2017). "Big data, platform economy and market competition: a preliminary construction of plan-oriented market economy system in the Information Era." World Review of Political Economy **8**(2): 138-161.

Wilman, F. (2020). The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US, Edward Elgar Publishing

4. AI & Civil Liability

4.1 Description of the issue

When dealing with novel fast-evolving technologies *that are deemed ever more complex, autonomous, capable of learning and modifying themselves, and thus opaque and unpredictable*[66], it is essential to assess the adequacy of civil liability rules.

However, in order to carry out such assessment, we must be able to identify the object of such assessment, as absent a clear definition of such it comes the impossibility to regulate. This results to be an obstacle, as there is no agreed definition of AI within the scientific community, except from the established fact that AI can have no agency[67]. The difficulty in defining such technologies can be tracked back to the fact that the term is used interchangeably to refer to technologies belonging to a variety of domains: cameras, fintech applications, toothbrushes, medical diagnostic solutions and smart home appliances are just a few examples[68]. The attempts that have been made to draw up a definition of artificial intelligence systems (AIS)[69], lack the necessary trait to discern across technologies due to the variety of the subject matter. As a result, there is a great deal of confusion regarding the scope of the normative

---

66 Expert Group on Liability and New Technologies (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies. Brussels, European Commission.

67 Wagner, G. (2019). "Robot, Inc.: Personhood for Autonomous Systems?" Fordham L. Rev **88**: 591.Also see Bertolini, A. (2020). Artificial Intelligence and Civil Liability. Bruxelles, European Parliament - Committee on Legal Affairs**:** 1-132.

68 Bertolini, A. (2022). "Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies." Europa e diritto privato(2): 369.

69 European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM/2021/206 final. Brussels, European Commission.

intervention, which poses a considerable challenge in developing appropriate regulation.

4.2 The current legal framework

Given that AIS are not beings but things, and more precisely products, the relevant European legal framework comprises mainly two bodies of norms, namely product safety regulation (§4.3), and product liability (§4.4).

4.3 Cont'd: Product Safety

Within the European Union (EU), product safety legislation is composed by the general rules as set out within the General Product Safety Directive[70] (the GPSD), and any other product or domain specific rules such as for medical devices[71], toys[72] or personal protective equipment[73] – to give just some examples. Under the general rules provided in the GPSD, it is a requirement to ensure that products[74] are safe, that consumers are informed of any risk associated to the use of a product – if any – and, to take corrective action in situations where a product is found to be unsafe.

---

[70] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002, 4–17

[71] 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.) *OJ L 117, 5.5.2017, p. 1–175*

[72] Consolidated text: Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (Text with EEA relevance) Text with EEA relevance.

[73] Regulation (EU) 2016/425 on personal protective equipment of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (with effect from 21 April 2018).

[74] Under art. 2(a) of the GPSD "product" is defined as "*any product - including in the context of providing a service - which is intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them, and is supplied or made available, whether for consideration or not, in the course of a commercial activity, and whether new, used or reconditioned.*"

Under art. 2(b) of the GDPS, a product safety is achieved when: *"[…] under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular: (i) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance; (ii) the effect on other products, where it is reasonably foreseeable that it will be used with other products; (iii) the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product; (iv) the categories of consumers at risk when using the product, in particular children and the elderly. […]*".

In addition, in order to prove conformity, firms may opt for the so-called presumption of conformity with EU legislation when they decide to use harmonized standards[75]. Standards are not binding unlike regulation, directives and national laws. However, their use can make it easier to demonstrate the safety of a machine or product, particularly when it comes to so-called "harmonized" standards. These standards are created upon request of the European Commission, and when manufacturers or other operators use them, it shows that their products adhere to the applicable EU laws. Furthermore, If a product belongs to those for which EU specifications exist, and affixing of the CE marking is mandatory, producers shall assess conformity with all the relevant requirements according to the appropriate procedure. CE marking indicates that the product has indeed been assessed by the manufacturer to check their compliance with the essential safety requirements set out by relevant legislation. Product certification rules thus serve a twofold aim: (i) they ensure high levels of product quality and safety, ultimately

[75] See art. 3(2) GPSD.

strengthening the users' confidence and protection, and (ii) create uniform procedures and market-conditions, allowing free trading of goods onto the EU market[76].

4.4 Cont'd: Product Liability

The framework for product safety is essential to ensure that products traded within the union are safe and will remain safe during the whole life cycle. The combination of mandatory guidelines and specification during the manufacturing and marketing phase together with the provision of administrative sanctions for non-compliance, provide for an ex-ante solution to product safety. This is then necessarily complemented[77] by the ex-post concept of product liability, which specifically addresses the question of who will bear the liability to compensate for a damage caused by products regardless of whether its commercialization was done in conformity with product safety rules.

Indeed, in the EU the Product Liability Directive (PLD)[78] provides for a horizontal mechanism where a producer will be strictly liable for damaged caused by defective products. As per the recitals in the PLD, the aim of this piece of legislation is that of ensuring consumer protection in an "*age of increasing technicality of a fair apportionment of the risks inherent in modern technological production*" by establishing "*liability without fault on the part of the producer*". Pursuant to art. 1 of the PLD "*the producer shall be liable for*

---

[76] European Commission (2016). The "Blue Guide" on the implementation of EU products rules. 2016/C 272/01. Brussels, European Commission.

[77] As provided by art. 17 of the GPSD, the GPSD shall apply without prejudice to the application of Directive 85/374/EEC. See also Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission.

[78] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal L 210 , 07/08/1985 P. 0029 - 0033

damage caused by a defect in his product.". The producers are identified under art.3(1) of the PLD as "*the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer.*". Furthermore, under art. 3(2), importers also assume liability, in that: "*without prejudice to the liability of the producer, any person who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business shall be deemed to be a producer within the meaning of this Directive and shall be responsible as a producer.*". Art.2 of the PLD then defines products in a very broad sense as "[…] *all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable. […]Product' includes electricity.*".

In relation to the concept of defect as referred to within the PLD, under art.6 of the PLD a product is deemed defective: "[…]*when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including: (a) the presentation of the product; (b) the use to which it could reasonably be expected that the product would be put; (c) the time when the product was put into circulation.*".

4.5 Cont'd: Civil Liability Regime for AI

Spanning out of the conclusion provided by the Expert Group on Liability and New Technologies[79], on 20 October 2020, the European Parliament (EP), approved and published a report containing a set of recommendations to the Commission on a Civil liability regime for artificial intelligence, thereafter, proposing the adoption of a new regulation (hereinafter CLR)[80].

[79] Expert Group on Liability and New Technologies (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies. Brussels, European Commission.

[80] European Parliament (2020). Civil liability regime for artificial intelligence. European Parliament resolution of 20 October 2020 with recommendations to the Commission

Firstly, under art. 3(a) the CLR provides a definition of AI- systems as being: "[...] *a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals*", autonomy identifies under art. 3(b) as being "*the ability to operate by interpreting certain input and by using a set of pre-determined instructions, without being limited to such instructions, despite the system's behaviour being constrained by, and targeted at, fulfilling the goal it was given and other relevant design choices made by its developer*".

Secondly, it creates two categories of risk. High-risk AI-system (under art. 4 CLR) as listed in the Annex will carry strict liability, while those not listed in said Annex will be considered low-risk and be governed by a fault-based liability (art. 8 CLR), coupled with a presumption of fault, and enumerated defences to the benefit of the claimant[81].

4.6 Major Challenges

Major concerns arise when one attempts to apply the existing legal framework to emerging advanced technologies and AIS. Some depend upon the general characteristics of existing and applicable legislation, primarily the PLD; some, instead, are specific to advanced technologies.

As per the former, the limited efficacy of the PLD is easily assessed by looking into the collected data regarding its application to date. The limited number of cases decided[82], as well as the circumstance that they cluster in domains where products are either not too sophisticated

---

on a civil liability regime for artificial intelligence (2020/2014(INL)). Brussels, European Parliament.

[81] See art. 8(2)(a) and (b) of the CLR

[82] See Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission. for a discussion please allow reference to Bertolini, A. (2020). Artificial Intelligence and Civil Liability. Bruxelles, European Parliament - Committee on Legal Affairs**:** 1-132.

(namely raw materials), or where a significant non-pecuniary loss is suffered (e.g., pharmaceuticals), typically associated to the infringement of a fundamental right of the user (typically health and life)[83], may be explained with the complexity of associated litigation[84]. Indeed, demonstrating defectiveness and the causal nexus between the defect and the damage suffered requires the acquisition of complex and thence costly evidence; such a concern is obviously going to be further exacerbated by increasing technological sophistication of the kind advanced technologies bring about. More broadly, the apparent technological neutrality of the legislation is clearly denied by the strong clustering of litigation in a very few, selected, domains, witnessing its intrinsic inadequacy to provide a general rule, applicable across the board to all sorts of products.

When advanced technologies are considered, instead, increasing automation brings about both additional material complexity, whereby the performance of tasks that used to be the sole competence of a human user is now often shared between humans and machines operating without direct supervision. This, in turn, also brings about the overlapping of different bodies of norms, also with respect to liability, that were not conceived to overlap, leading to the multiplication of potential responsible parties, thence ultimately to cases of alternative causation. To exemplify, in a car accident involving two traditional vehicles either one of the drivers will be responsible. Residually, a – rather clear – malfunctioning in the vehicle might become of relevance, however accounting for a very small percentage of the overall

[83] Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

[84] Bertolini, A. (2020). Artificial Intelligence and Civil Liability. Bruxelles, European Parliament - Committee on Legal Affairs**:** 1-132.

occurrences. When increasingly autonomous vehicles are concerned, instead, many more layers of complexity are added. Firstly, the driving task will be shared between the human driver and the machine. With current levels of automation, the human will be in control most of the time, while, in some instances, will relinquish control to the vehicle itself. Even such a choice, to activate the autonomous function, will be that of the human user, and potentially trigger his responsibility for a faulty choice, similarly to the incapacity – eventually due to distraction – to resume control if prompted to do so. Moreover, an autonomous vehicle will also be a connected one. Therefore, the accident might also be due to the road infrastructure or to the faulty connection between that and the automobile. So briefly sketched, the liability framework might point to different forms of responsibility, due to a variety of applicable legal rules, including the fault-based liability of the driver, the – typically strict – responsibility of the owner, the – potentially semi-strict – responsibility of the manufacturer, the – possibly contractual – responsibility of the different service providers involved. The overlap of so many different rules, pointing at equally different responsible parties, increases the cost and complexity of litigation, in particular with respect to the exact assessment of the causal nexus[85]. That, in turn, could lead to a lack of internalization of costs by the parties that are either responsible or best suited to manage and insure against such costs, leaving the burden on the weaker party[86], eventually discouraging access to justice[87]. Ultimately this could lead to distrust on the side of the users towards advanced

[85] For a detailed analysis, see Bertolini, A. and M. Riccaboni (2020). "Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules." European Journal of Law and Economics: 243.

[86] Bertolini, A. (2022). "Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies." Europa e diritto privato(2): 369.

[87] Expert Group on Liability and New Technologies (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies. Brussels, European Commission, Bertolini, A. (2020). Artificial Intelligence and Civil Liability. Bruxelles, European Parliament - Committee on Legal Affairs**:** 1-132.

technologies, due to the legal risks associated with their uptake, discouraging their penetration in the market[88].

Within such an overall framework, current product liability rules prove particularly problematic. Indeed, complex and costly litigation of the kind required by the PLD, witnessed already today in less technologically sophisticated domains, are only doomed to worsen as soon as AIS are considered. Apparent technological neutrality will most certainly fail with increasing automation in providing a one-size-fits-all solution to the problem.

Finally, the most recent proposals specifically dedicated to AIS and civil liability (e.g., CLR) seem to move along similar lines, by advancing a horizontal approach to regulation, applicable – despite with different regimes (either strict or fault-based, depending on the anticipated level of risk) – to a very broad notion of AIS. Instead, to, all those domains (e.g., medical malpractice, capital markets and investment law, the liability of professionals, of keepers of things in custody, of owners of vehicles, as providers of consumer products and services, to name a few) are separately regulated with equally different incentive structures and rules. All major criticism that could be brought to said proposals ultimately stems from such a consideration[89].

4.7 Recommendations

Some very fundamental recommendations may be here formulated, based on the synthetic analysis provided.

---

[88] Bertolini, A. and M. Riccaboni (2020). "Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules." European Journal of Law and Economics: 243., p. 269

[89] For a detailed analysis of all potential criticism to the CLR please allow reference to Bertolini, A. (2022). "Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies." Europa e diritto privato(2): 369.

1. Civil liability arising from the use of emerging advanced technologies, including AIS needs to be regulated in as much as it affects the incentives towards the use and uptake of said products and devices.
2. However, the intrinsic technological diversity, as well as the equally different domains of use of technologies, also reflecting on the diversity of the – professional and non-professional – users thereof necessarily require a technology-specific approach to regulation. No one-size-fits-all solution could effectively regulate all AIS, without leading to either the under-protection of certain users – not possessing adequate knowledge and economic resources to initiate litigation – or the over-deterrence of other professional-users in adopting more technologically advanced solutions.
3. Regulatory efforts should be focused on those domains that already demonstrate the likelihood to transition towards higher levels of automation and technological sophistication. Those include, despite not being limited to, the medical profession, road vehicles and capital markets.
4. All regulatory efforts in the domain of civil liability should prioritize the internalization of costs by those that (i) develop and (ii) use the technology considered. This entails focusing on the compensatory nature of liability rules, rather than the exact assessment of responsibility or fault.
5. This in turn entails favoring a one-stop-shop approach whereby the responsible party is clearly identified ex ante, by imposing a strict liability upon that very party, minimizing if not overall eliminating the need to specifically assess the existence of a causal nexus. Alternative causation scenarios need to be radically excluded through such kind of rules.

6. Distribution of costs along the entire value chain are better addressed through secondary litigation, once the victim was compensated.
7. Ex ante investments in safety are better ensured through product safety regulation, rather than ex post liability rules, which show little or no effectiveness in inducing a desired behavior ex ante.

Bibliography

Bertolini, A. (2020). Artificial Intelligence and Civil Liability. Bruxelles, European Parliament - Committee on Legal Affairs**:** 1-132.

Bertolini, A. (2022). "Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies." Europa e diritto privato(2): 369.

Bertolini, A. and M. Riccaboni (2020). "Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules." European Journal of Law and Economics: 243.

Ernst&Young, Technopolis and VVA (2018). Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Brussels, European Commission.

European Commission (2016). The "Blue Guide" on the implementation of EU products rules. 2016/C 272/01. Brussels, European Commission.

European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM/2021/206 final. Brussels, European Commission.

European Parliament (2020). Civil liability regime for artificial intelligence. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). Brussels, European Parliament.

Expert Group on Liability and New Technologies (2019). Report on Liability for Artificial Intelligence and other emerging digital technologies. Brussels, European Commission.

Timan, T., R. Snijders, M. Kirova, S. Suardi, M. v. Lieshout, M. Chen, P. Costenco, E. Palmerini, A. Bertolini, A. Tejada, S. v. Montfort, M. Bolchi, S. Alberti, R. Brouwer, K. Karanilokova, F. Episcopo and S. Jansen (2019). Study on safety of non-embedded software. Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems: final study report regarding CAD/CCAM and industrial robots. Brussel, European Commission.

Wagner, G. (2019). "Robot, Inc.: Personhood for Autonomous Systems?" Fordham L. Rev **88**: 591.

5. About the European Centre of Excellence on the Regulation of Robotics and Artificial Intelligence (EURA)

The EURA Jean Monnet Centre of Excellence constitutes a focal point of competence and knowledge on Robotics and AI, focusing on their ethical, legal, social and economic (ELSE) implications.

EURA's mission is to promote innovative multidisciplinary research, offer advanced educational programs, and foster the dialogue with policy makers, increasing social awareness and promoting an informed debate.

Through its activities, as well as its interdisciplinary and functional-based approach, EURA creates a worldwide network of experts, professionals, stakeholders, and policy makers, facilitating cross-fertilization among different fields and interest groups.

Ultimately, EURA intends to identify, assess, discuss, and promote the European Approach to AI and advanced robotics, as defined by European Commission in its communication of the 25th of April 2018.

5.1 Mission

The EURA Centre of Excellence has four main goals.

Firstly, through the organization of workshops, conferences and other events involving leading international experts, it creates a multidisciplinary community and advances the academic debate, allowing the early-on identification of relevant social and policy issues.

Secondly, the Centre offers a wide variety of advanced educational programs, such as PhD level courses, Summer Schools, and Boot Camps, which provide academia-oriented students with the knowledge and methodology necessary to carry out innovative research in the field, and deliver readily applicable and immediately relevant information for

businesses and investors intending to bring R&AI applications to the market.

Thirdly, EURA fosters the dialogue between academia and policy makers. Indeed, officials of national, European and International Institutions are regularly invited to take part to the activities organized by the Centre; at the same time, they are directly addressed through the yearly policy paper, which aims at providing EU and international policy-makers with the early identification and assessment of socially and politically relevant issues, as well as with proposals for actions to be taken.

Lastly, the Centre intends to increase social awareness and encourage an informed debate among society at large. Through our interactive website, citizens can find informative content and interactive tools to pose questions and advance concerns, ultimately engaging into an informed and fruitful dialogue.

5.2 Departments and collaborating institutions

EURA is hosted by the Scuola Superiore Sant'Anna, a public university institute - with special autonomy - working in the field of applied sciences: Economics and Management, Law, Political Sciences, Agricultural Sciences and Plant Biotechnology, Medicine, and Industrial and Information Engineering. The School promotes the internationalization of didactics and research with innovative paths in the fields of university education, scientific research and advanced training.

The departments collaborating in EURA are the DIRPOLIS Institute, the BioRobotics Institute, the TeCIP Institute, the Institute of Economics, The Institute of Management, the Department of Philosophy at the University of Vienna and City Law School, University of London.

Moreover, EURA benefitted from the structured collaboration of experts from the Department of Philosophy of the University of Vienna,

Prof. Mark Cockelbergh, and London School of Economics and Political Sciences, Prof. Luke McDonagh.

EURA also benefitted from the collaborations with other research centres such as Research Centre of European Private Law (ReCEPL) and European projects Inclusive Robotics for a better Society (INBOTS), PErsonalized Robotics as Service Oriented applications (Perseo), RegulAIte.