H2020-SC1-DTH-2018-2020

Type of Action: RIA Research and Innovation action

Topic: Adaptive smart working and living environments supporting active and healthy ageing

Grant Agreement no: 826266

Deliverable

D2.4 Ethical Issues in Adaptive Systems for Active Ageing

COADAPT

Start date of the project: December 1, 2018 Duration: 42 months

Project funded by the European Commission within the Horizon 2020 programme for research, technological development and demonstration		
Dissemination Level		
PU	Public, fully open	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	□
CL	Classified	□

Notices

For information, please contact the project coordinator, Prof Giulio Jacucci, e-mail giulio.jacucci@helsinki.fi

This document is intended to fulfil the contractual obligations of the CO-ADAPT project, which has received funding from the European Union's Horizon 2020 Programme, concerning deliverable D2.4 described in contract 826266.

Table of Revisions

Version	Date	Description and reason	Author	Affected sections
v0.1	September 2020	Providing initial content	UNIPD	ALL
V1.0	End of November 2020	Drafting the final version based on partner' feedback	UNIPD	ALL

Partners

1 HELSINGIN YLIOPISTO (UH)

2 TYOTERVEYSLAITOS (FIOH)

3 INNOVATION SPRINT (INNO)

4 UNIVERSITA DEGLI STUDI DI TRENTO (UNITN)

5 UNIVERSITA DEGLI STUDI DI PADOVA (UNIPD)

6 IDEGO SRL (IDEGO)

7 BNP SRL (BNP)

8 AALTO KORKEAKOULUSAATIO SR (AALTO)

9 ETSIMO HEALTHCARE OY (ETSH)

10 ELECTROLUX ITALIA SPA (ELUX)

Authors

- Professor Luciano Gamberini (UNIPD)
- Professor Anna Spagnolli (UNIPD)
- Patrik Pluchino (UNIPD)
- Chiara Rossato (UNIPD)

Reviewer

- Professor Giulio Jacucci (UH)

List of Abbreviations

I4.0 - Industry 4.0

IoT - Internet of Things

CBS - Cyber-Physical Systems

AAT - Ambient Assistive Technologies

GDPR - General Data Protection Regulation

OECD - Organization of Economic Cooperation and Development

AI - Artificial Intelligence

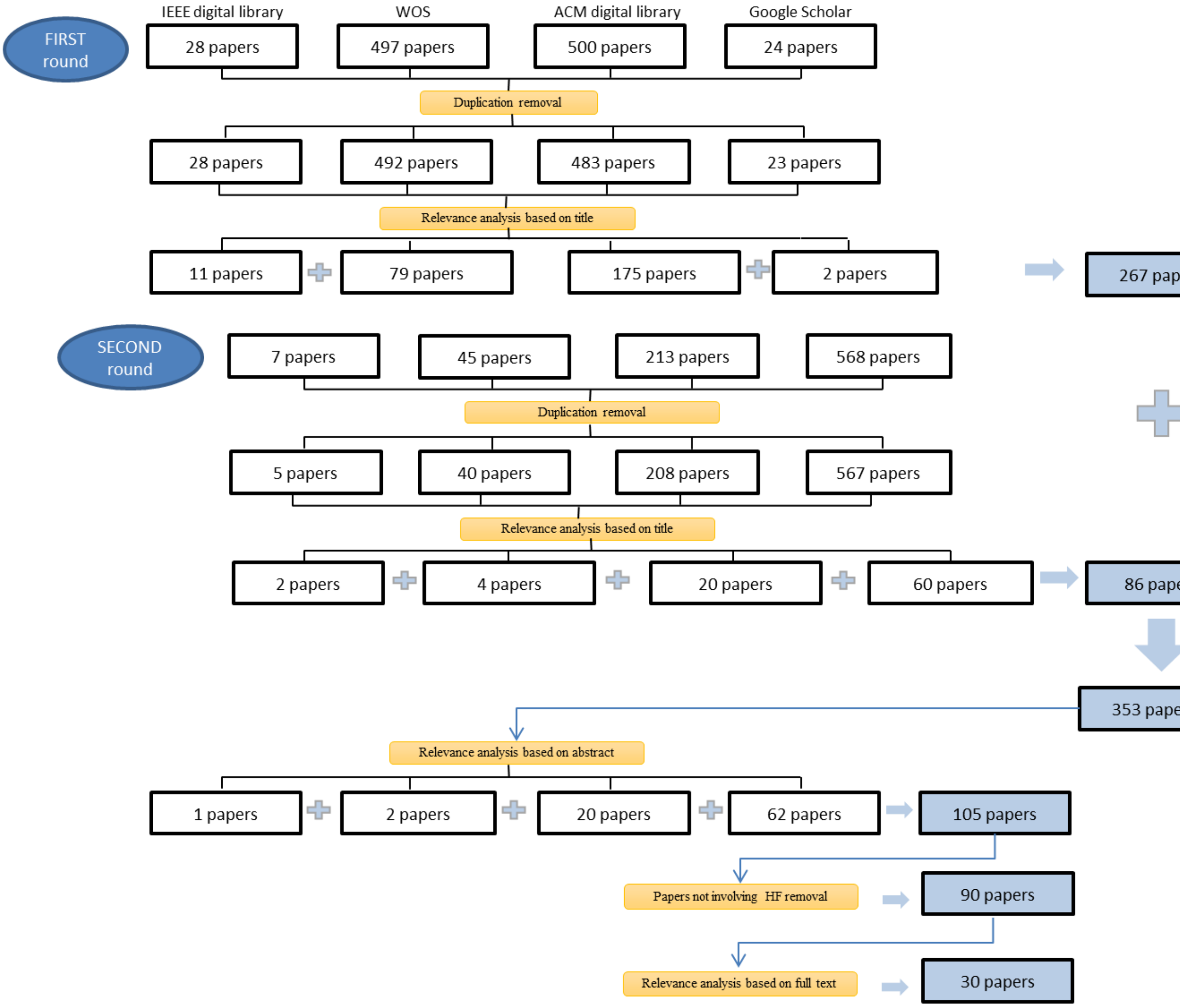
LoA - Level of Autonomy

I5.0 - Industry 5.0

VSD - Value Sensitive Design

IAS - Intelligent Autonomous Systems

List of Figures



List of Appendix

Table of contents

Executive Summary

Adaptive systems such as the CoAdapt assembly workstation, are spreading in the context of Industry 4.0 to improve performance and support the operators. At the same time, however, ethical and privacy-related concerns can be raised by the fact that such systems monitor the operators and intervene in the work process according to automated actuation criteria. The risk is to undermine the users' control and self-determination, dignity and autonomy, and to increase socio-economic disparity. Moreover, such concerns can impact the users' trust and behaviour towards the system.

This document reviews the scientific literature on the ethical and users' concerns raised by adaptive systems. After explaining the literature review method adopted, this document describes in details the nature of those issues and concerns. The document concludes by outlining some guidelines to lessen real and perceived ethical threats, favour acceptance and increase the workers' awareness.

1 Objectives

WP2 aims to ensure the technology solutions developed in CO-ADAPT are accepted by users, reflect their views and needs, are usable and respectful of ethics. This is a step beyond pursuing the mere formal compliance with ethical regulation, since it means to ensure that users perceive that the adaptive system does not represent a threat to them. The purpose of the present deliverable is to review the users' concerns about adaptive systems as they are reported in the literature and which undermine their trust and acceptance. The final purpose of the document is to extract from this literature the general recommendations that can inform Co-Adapt developers.

2 Introduction

The adoption of smart technologies and intelligent objects exchanging information with each other and managing large amounts of data is part of the workplace innovation spreading within Industry 4.0 (I4.0; Cohen et al., 2019). Internet of Things (IoT; interconnected objects based on internet protocols and network technology enabling communication; Wortmann and Flüchter, 2015), and Cyber-Physical Systems (CPS; physical and engineered systems with computing and communication capabilities to monitor, coordinate, control and integrate multiple operations; Rajkumar, et al., 2010) are some of the original components of such environments (Evjemo et al., 2020) which determine the advancement of so-called intelligent manufacturing (Zhong et al., 2017). In this context, the physical devices are closely connected with computer systems and humans, in a continuous, daily exchange of information and interactions. The development of such kinds of systems represents a crucial step forward in the process of human centralization in manufacturing work environments: the operator is more and more involved in the interaction with the machines to gather more and more bolster from them (Romero at al., 2017). This kind of interaction calls for an accurate consideration of the acceptability of the new situation from the worker, considering also the increment of workload required to her/him (Belkadi et al., 2020). Indeed, whilst these innovations enable the companies to meet the productivity requirements of the market, from the other side they increase the complexity of the workplace (Longo, Nicoletti, & Padovano, 2017).

The proper implementation of such systems may result in a more aware support of the worker through these systems' ability to identify the actual situation requirements, and thus taking the most appropriate actions (Belkadi et al., 2020). Such technologies are adaptive and flexible, able to coordinate their actions with those of humans, to meet their specific needs, and to solve intervening problems (Peruzzini and Pellicciari, 2017). Peruzzini and Pellicciari pointed out how adaptive systems demonstrated their suitability in supporting the aging workers' issues due to physical and cognitive function decreases. To this aim, the machines are designed to be context-aware and base their behaviours on defined adaptive rules. The system's adaptivity stand on its capability to automatically change its structure, functionalities, or interface based on the differing needs of individual or groups of users over time (Benyon, Innocent and Murray, 1987). To do so, adaptive systems rely on *models* describing which physical and logical features the system can alter (domain model), based on which users' characteristics (user' model). The combination of these two models results in *interaction model* including inferences, evaluations, and adaptation mechanisms (Benyon and Murray, 1993). The user model is developed and enhanced by monitoring the interaction, and thus by monitoring the user. The interaction may involve both implicit and explicit modes to acquire information needed for the development of the models. The explicit acquisition mode may include some co-operative behavior on the users' side, such as providing information. The implicit acquisition mode consists of acquiring data on the users' state, e.g. inferences generated by data on the users' physiological signals. While implicit data collection allows less intrusive and fine-tuned real-time adaptation, it also raises critical issues about ownership and control over the mechanism of data collection (Schaub, 2018; Fairclough, 2009). Moreover, users develop more expectations on an adaptive system, and therefore more likely to be frustrated when the application does not work as they expected, which might also undermine trust (Gena, 2005). Fear of a potential harm to psychological and/or societal well-being, may prevent the acceptance of the system (Gervasi, Mastrogiaconno and Franceschini, 2020). Gervasi and colleagues pointed out that the more autonomy the machine, the higher the level of risk/vulnerability for the user is, especially whether a strong trust relationship has established. Computer ethics has to address the task of protecting users in both their ethics and feeling that their privacy and needs are respected by the machine. This poses the basis for its acceptance or not (Reynolds and Picard, 2005).

A balanced mutual human-machine awareness could develop the interaction towards a dyadic relationship more and more collaborative and symbiotic able to support the users more efficiently (Klein et al., 2004; Jacucci et al., 2015). Technology designers have a critical responsibility in this respect as they have to exploit solutions which would be human-values sensitive and aware of the context of use (Albrechtslund, 2007). The ethical principles guide the distinction between right and wrong and help in the protection of human rights (Singer, 2011). In the context of technology design, these ethical principles are translated into a series of design guidelines aiming at respecting the principles of fairness, honesty, trustworthy and privacy respectfulness (Preece, Sharp and Rogers, 2015). First of these guidelines regards the limitation of data collection to the only necessary information to prevent the acquisition and processing of sensitive and unnecessary data. The four main principles accountable for the development of a computing system refer to the impartial user's treatment (*Fairness*), the visibility of the decisions that the system makes (*Transparency*), the availability of explanation for the system decision to prove their accuracy and correctness (*Accountability*), and the understandability of those explanations (*Explainability*). These principles are even more relevant when the machine is able of autonomous decision-making (Gervasi, Mastrogiaconno and Franceschini, 2020).

3 Method

The research questions that have driven this literature review are the following:

1. What are the principal themes and issues discussed in literature about users' concerns regarding adaptive systems and the ethical privacy issues related to the interaction with such systems?
2. Which are the guidelines/recommendations regarding ethical and privacy issues, to consider in the design and implementation of adaptive systems, especially in the working environment?

The literature review was organized considering the main research topics: adaptive systems; users' data concerns about privacy and ethical issues; the ageing factor of the user. The searching keywords were "adaptive environment", "adaptive system", "adaptive assembly workstation", "ethics", "user trust", "active ageing", "implicit data" and some variations; keywords combinations including “industry”, “manufacturing”, “workplace” were also used. The scientific databased considered were the ACM Digital Library, the Web of Science, IEEE Xplore Digital Library, and Google Scholar.

The bulk of 353 papers obtained with keywords search was then filtered for relevance based on title and abstract, at first, and the on the full text. Thirty papers survived this selection. A graphical representation of the review procedure is depicted in Figure 1.

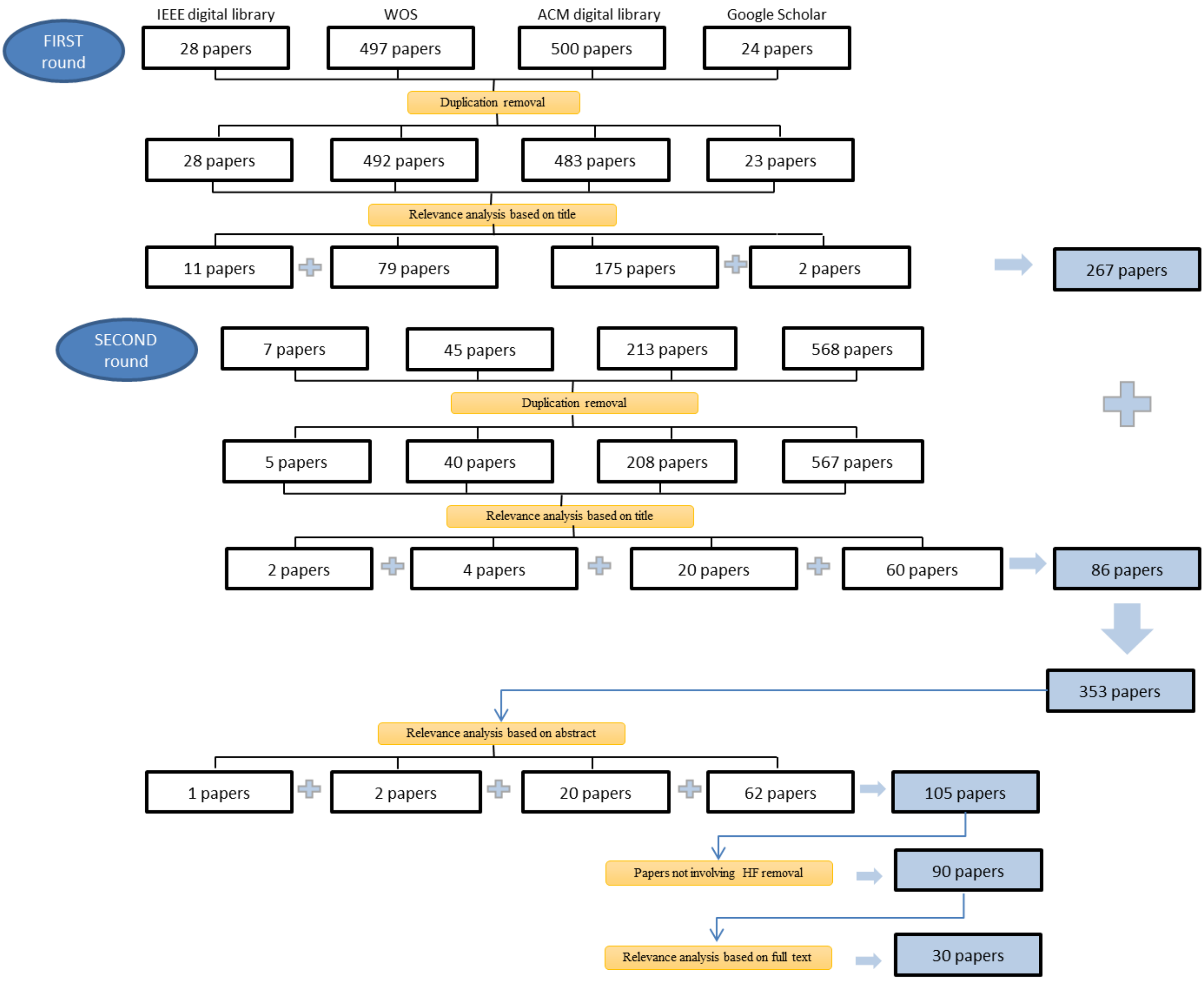


Fig. 1 Search process

The table in appendix 1 summarizes, for each paper, the type of technological system assessed, the specific aspects of the systems that arise issues/concerns, the application fields, the consideration of trust explicitly. The papers cover a period of 17 years (Figure 2).

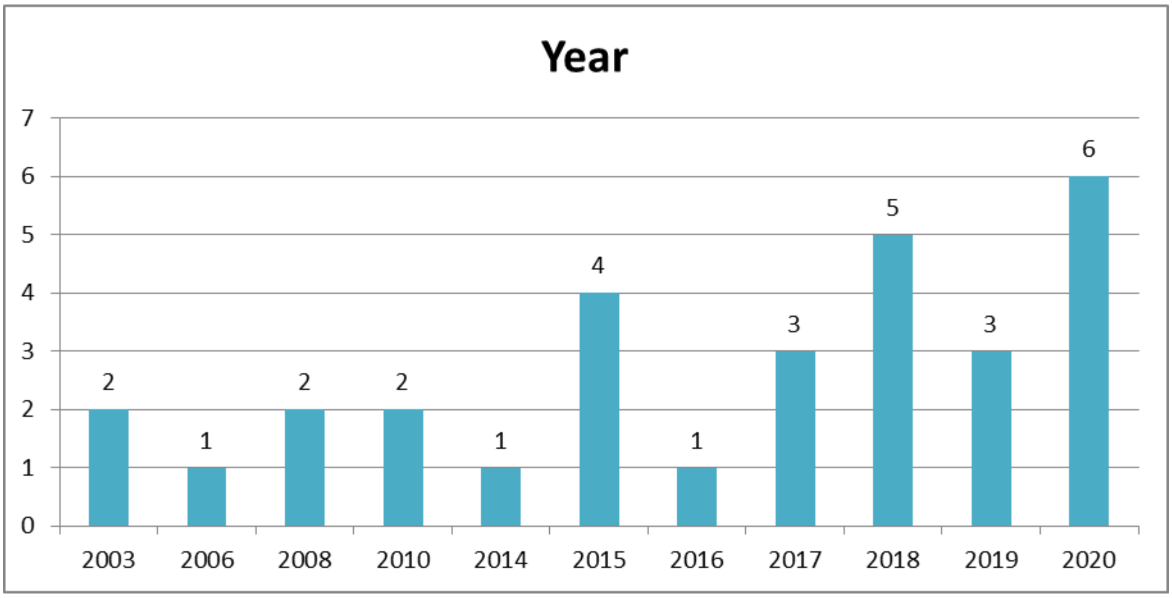


Fig. 2 Number of publications per year

Of the thirty papers considered, twelve papers have considered the issues of use adaptive systems within industrial working environments specifically. Eight papers discussed directly the cyber-physical systems or symbiotic systems. Robotic systems are considered explicitly in seven publications from which emerged the extent of societal impact derived from the adoption of such technologies in human life. The ethical implications derived from adaptive systems adoption are the focus of twelve papers reviewed. The specific concerns they have focused on are ethics at large, intrusiveness, privacy, transparency, trust, and users' preferences (Figure 3).

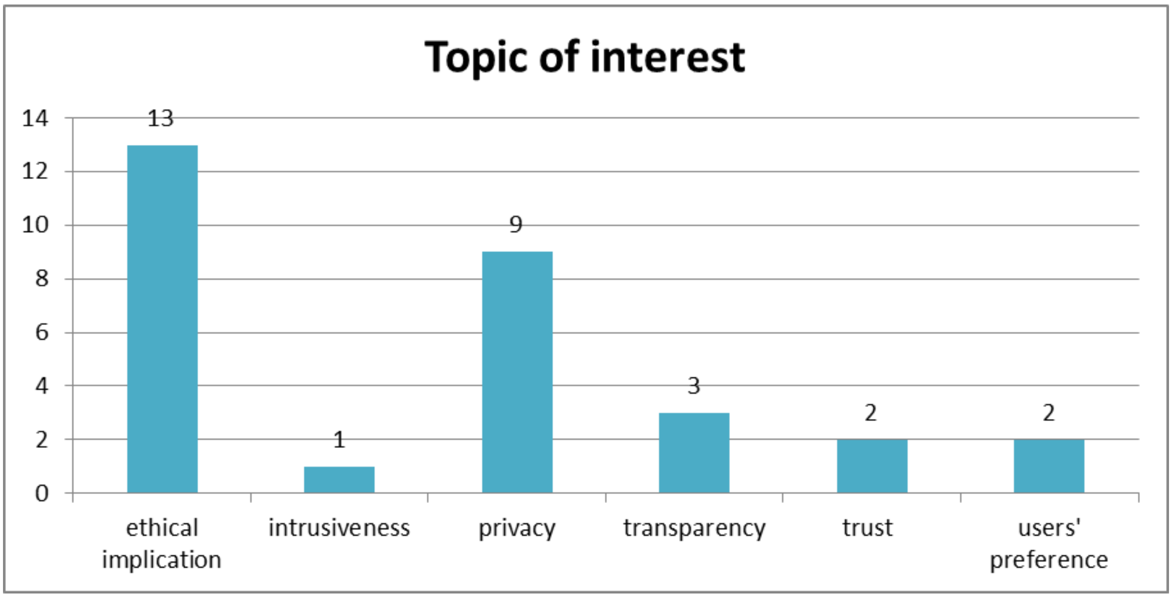


Fig. 3 Number of publications per topic of interest

4 Results

This section describes the users' concern and the ethical concerns highlighted in the literature collected according to the process described in the previous section. Section 5 instead will distill some guidelines to reduce those issues and concerns.

4.1 Users' related issues and concerns

The analysis of the literature revealed two principal sources of individual's concerns related to the use of adaptive systems: the process of data monitooring and the ensuing modality of supporting the users.

4.1.1 Monitoring

a. Privacy concerns

One of the main concern relating to the adoption of intelligent adaptive systems regards the protection of personal information relating to the risk of users' data misuse or usurpation (Spagnolli et al., 2016; Schülke et al., 2010; Kobsa and Schreck, 2003; Lee and Kobsa, 2017).

Spagnolli (Spagnolli et al., 2016) discussed the risks related to the adoption of symbiotic systems with ethics, information security, law, and human-computer interaction experts. Symbiotic systems represent the close relationship between human users and machines in which the information exchange happens transparently and unobtrusively through a procedure of implicit collection of the user's data (e.g., by sensors). The data become informed about the needs of the individuals upon which the machine can develop a users' model and make decisions to provide the most appropriate service to him/her adapting its functioning. In such close interaction, the risks of information leakage and malicious user profiling are concrete, as well it is the risk for deceitful use of data and threat to information security.

The authors pointed out some practices to face these concerns. First of all, they suggested to embody in the system design the society values (e.g., honesty, equity, self-determination, dignity, and freedom) and domain-values (such as network security, user-centeredness, transaction fairness, transparency, identity, and data protection). Also, the *education* of users should make them understanding the risks of the technology and the procedure to minimize them. As well, the *regulation* of collection and treatment of data should be provided. Finally, an agency, namely *Watches*, representing the users' rights should be responsible for the promotion of e*ducation* and r*egulation* practices, for the monitor of ethical risks, and for the certification of the procedures.

In the context of symbiotic interaction form, Jacucci and colleagues (Jacucci et al., 2015) depicted the condition of interdependence between humans and machines from a user-centered perspective. The authors highlighted the requirements of these systems, namely the transparency, reciprocity, and collaborative use of the resources between machines and humans. This kind of interaction would protect both the goal independence of the two agents involved and specifically the human still enhancing his/her capacities. Indeed, even if the symbiotic systems collect users' data to support them and improve their performance, this process may produce ethical risks related to the protection of personal data. These risks involve losing control and agency over their data by the users and are specifically related to the implicit form of data collection and the process of data filtering performed before to transmit the deriving information to the users.

The concern about (implicit) physiological data acquisition through systems equipped with sensors is reported also in the context of usage of Ambient Assistive Technologies (AAT) for the health monitoring of fragile individuals. Schülke, Plischke and Kohls (Schülke, Plischke and Kohls, 2010) discussed the impact on the seniors' life of such technologies aiming to monitor health status and assist the users in the case of necessity to allow them to independently live in their own homes as long as possible). Despite the general accordance and recognition of the benefits of AATs, especially in their capacity to communicate with relevant figures for the users (e.g., medical professionals, family members) which facilitate the senior’s social interaction, the authors collected from their users' worries about the possibility of privacy violations. These worries impact users' acceptance of the system's constant monitoring even if for their benefits. Moreover, in this kind of situation, the concerns about the social effect of the usage of AATs are related to the worries that they could replace real interpersonal contacts.

As well, the privacy issues due to the collection of personal data represent a critical concern also in the context of Industry of the Future where cyber-physical systems able to collect workers' data are employed to augment operator's capabilities. Longo and colleagues (Longo et al., 2020) found that these concerns may produce resistance to the acceptance of such kinds of systems by workers, especially among those with an old mindset or with work-related stress.

According to Kobsa and Schreck (Kobsa and Schreck, 2003), personalization benefits may decrease whenever the user perceives some privacy risks in the process of users' data collection of an adaptive system. The individuals’ trust in the anonymization processes of their data is crucial for an efficient interaction. The authors, however, observed that users' demands regarding privacy policies depend on several individual factors: general preferences for privacy (e.g., whether anonymous or identifiable use of information systems is preferred); desire to keep different type of characteristics apart from each other (e.g., whether different applications may only share a small or rather a large part of the personal data in a user model); personal roles that a user assumes when interacting with user-adaptive systems (e.g., that of a company employee at work or a private citizen at home); and extend to which the benefits that user-adaptive systems are appreciated (e.g., a trade-off between added value of personalization and disclosing personal information). Overall, the authors observed that user interaction with the system results in a more extensive and frank in the case of data anonymization. The personalization experience improves furthermore, as the possibility to conceal their identities seems to alleviate users’ privacy concerns whilst preserving the benefits of personalized interaction.

Besides the individual preference about privacy safeguards, Lee and Kobsa (Lee and Kobsa, 2017) pointed out the importance of contextual information on the risk perception and decision making related to personal data protection. They observed that users' perception of privacy risks related to the use of Internet of Things technologies that collect massive amounts of personal information are influenced by the specific place where the user is, as well by the identity of information requester, and by the modality, reasons, and duration of data monitoring processes. This could have serious consequences on the subsequent decisions users made about privacy policy. It appears that the monitoring of personal data in a private place is wide more unacceptable than in semi-public spaces (e.g., restaurant), even if other factors influence the user's behaviour in this environment. Indeed, monitoring modalities may reveal personal information directly (e.g., monitoring of eye-movements to detect where they are looking), even if it is purposely, is perceived more unacceptable than providing information about their personal devices (e.g., unique phone identifier), presumably since it is perceived not to be directly connected to their behavior. Moreover, the unknowing of the information requester identity elicit more privacy-conservative behaviours, as well the possibility that school personnel and/or employers may gather such personal information and behaviours. Regarding the potential reasons for personal data monitoring, the authors reported that between safety, commercial, social, convenience, and health reasons, participants consider monitoring as very unacceptable when it is performed for social or safety-related purposes (at least whenever the context is perceived as safe), while health is considered the most significant purpose. The persistence of monitoring activities elicits different levels of acceptance as well: continuous monitoring is related to higher concerns about the risk of privacy violations.

Therefore, the benefits of IoT applications are exploitable in numerous fields since their differential capacities in environment interaction in the function of the related type of data managed, data entry, data sharing, learning, and decision making processes. Nevertheless, these specific characteristics that make them adaptive make also more relevant the need for finding a balance between the privacy of users and the benefits related to such devices (e.g., real-time responses, improved accessibility and controllability of devices, increased efficiency, and productivity). Weinberg and colleagues (Weinberg et al., 2015) identified specific concerns related to these advantages, concerning both the service providers and technical aspects (e.g., interoperability, communication, and standards), and the users, namely the privacy and security issues. The high amount of users’ data generated, stored, and processed, most of which are sensitive and more susceptible to hacking threats and the loss of privacy, require to IoT-based systems stronger measures to protect the users.

b. Awareness and Understanding

Behind the implementation of strategies for users' data and privacy protection, from this literature analysis emerged the necessity of providing users with the appropriate means to be aware of the risks related to the use of an adaptive system. In four of the reviewed studies, the main aim was to assure that individuals possess the appropriate information about the privacy concepts and protection mechanisms relating to the processing of their data by the system (Mannhardt et al., 2019; Hamidi et al., 2018). The insufficiency or incorrect users' understanding of the system functioning, with specific regards to the modality of data collection and utilization, may result in an underestimation of the privacy risks by the users themself (Knockaert and De Vos, 2020; Van De Garde-Perik et al., 2008).

In the context of smart manufacturing, Mannhardt, Petersen and Oliveira (Mannhardt et al., 2019) aimed to increase the workers' privacy awareness about the process of data collection made by wearable sensors to support them during the advanced working activities. A better understanding of privacy concepts had a positive impact on the users' trust in smart manufacturing systems. The provision to the operator with privacy guidelines related to the actual phase of data processing increased the perceived relevance of the privacy principles stated in GDPR (European Union, Regulation (EU) 2016/679, 2016). More interestingly, it emerged that changing the perspective of the responders, from an operator's to a manager's point of view, and considering different stages of data processing (e.g., logging to the system, data mining), the perceived relevance of the diverse principles changed. The perceived relevance of these principles should improve making more comprehensible to the operators the trust and privacy concepts related to their data acquisition by smart sensing technologies during working activities. As a consequence of this also of the operators' agreement on the adoption of smart systems would improve.

It is observed by van de Garde–Perik and colleagues (van de Garde–Perik et al., 2006) a similar result also in the context of health monitoring in Ambient Intelligent systems. They observed that people may consider the diverse Organization of Economic Cooperation and Development (OECD) guidelines (i.e., concerning the general guidance for the collection and management of personal information) with different relevance on the base of the main concerns they have. The authors derived four clusters of people: people consider most important to know the purpose for which data is collected (i.e., purpose); people who consider critical to know which other parties have access to the data, and to be assured that the data is protected by security safeguards, and to be allowed to access to the data themselves (i.e., guarantees existence); people who particularly value to have access to and control over their data (i.e., data control); people who especially care about the type of data that is collected, and want to be able to inspect those (i.e., type of data).

A critical finding related to different relevance attributed to privacy risks is reported by Hamidi and colleagues (Hamidi et al., 2018). They observed that the users may be more trusting, and more prone to overlook privacy risks and maintain a positive attitude towards adaptive technologies in contexts where the aim is to assist users than in non-assistive context. The authors annotated that the users of adaptive assistive technologies valued the tracking data as effective to support self-monitoring. Nevertheless, they also addressed that, when explicitly inquired, users reported serious concerns about privacy risks regarding online personal data collection. These concerns regard especially the identity of who could access their data and how they will be utilized (i.e., privacy threats unawareness, and identification threats). It emerged that many of such concerns derived from news stories on popular platforms about data leaks. In concluding, the participants expressed a strong preference to be informed about how their data will be used (unawareness threat) and to be anonymized when the data would be shared outside their family or medical circle (identification threat). Overall, the study underlined the need to consider and minimize multiple privacy threats (e.g., non-repudiation, noncompliance). Besides, in contexts where the adaptive systems assist fragile users, as in the case of adaptive assistive technology, specific consideration of the actual users' awareness about the privacy risks is necessary.

Furthermore, the need to be aware and understand the functioning of data collection and transmission was particularly relevant in the case of processing of special categories of personal data that require explicit user's consent, such as the biometric data for a person's identification. Knockaert and De Vos (Knockaert and De Vos, 2020) observed that the main concerns reported by the users regard the knowledge of the time period of data collection and of the mean by which this occurred (e.g., photo, voice recording), and if the data collection would be continuous or not, whether specific behaviour may be avoided to not affect the data collection, and finally, who can have access to the collected data. This information may be included in the consent provided to users when they are going to use systems to be ethically and really "informed". Gathering sufficient information about which data would be utilized and in which way the output based on them would be determined is required to assure users of the possibility of an informed decision about the system in use. The requirement to have the appropriate information to understand the system functioning derived also from the observation that the transparency principles (i.e., stated in the GDPR, like the right, for the data subject, to receive information, and a corollary obligation for the data controller to provide them in a clear and plain language both at the beginning and all along with the processing of personal data) may fail whether the user does not understand the information provided. Knockaert and De Vos highlighted that such uncertainties may arise anxiety about the system and that they are to be considered to ensure the right to be properly informed and the very use of the system. Thus, it would be foreseen the possibility to provide additional information by request, to avoid discriminatory system use.

Moreover, an inappropriate or insufficient understanding of the privacy and ethical risks related to intelligent technologies/ambients with the capacity to collect users' data implicitly, may also result in a discrepancy between users' privacy attitudes as they may assert and their actual behaviour, likely less responsible. Van De Garde-Perik (Van De Garde-Perik et al., 2008) reported this occurrence in the context of a personalized recommender system towards which the users behaved risky, showing a tendency to disclose personal information even whether they explicitly evaluated it as sensitive (to be protected) and have claimed to have balanced costs against the benefits of disclosure.

In such considerations, the call for appropriate transparency features embedded in adaptive systems able to modify their characteristics in response to the information gathered from the users appear as crucial. Transparency refers to the extent to which the system discloses criteria of its functioning, thus the extent to which a machine provides the human with information about itself and its functioning (i.e. all or part of its model, the common objective). It is very important to ensure the human does not misunderstand current and future machine behavior and to enable users to operate a given system effectively, easily, and responsibly (Spagnolli et al., 2018; Pacaux-Lemoine and Trentesaux, 2019).

The importance of making users understanding and aware of the functioning of systems able to adapt autonomously on the base of data obtained implicitly from the users was carefully considered in the context of symbiotic systems and Artificial Intelligence (AI). Experts' opinions in this regard were collected by Spagnolli (Spagnolli et al., 2018) and underlined the cruciality of determining genuine transparency in such systems to protect the users from unethical usage of their data and to make them able to make informed decisions about data to input into the system and which would be used by the system to provide outputs. The extent to which the system provides the criteria of its functioning, i.e., transparency, would allow the users to use it responsibly. Several challenges arose regarding how transparency may be achieved in a way caring for users. Indeed, this discussion pointed out the issues about which information to provides to users and how to make it understandable and usable to avoid users' negligent behaviors, and to help them remain consistent with their values. In such a way, it would be avoided situations of the power imbalance between humans and machines, of users' trust in the system decrement, of “manipulative” actions by the system (e.g., manipulative recommendations). To make the transparency really “enabling” the users should be provided with understandable information, limited in the amount of those really necessary and connected to users’ goals, priorities, and responsibilities. Cramer and colleagues (Cramer et al., 2008) pointed out that recommendations systems improve their efficacy when the users understand its functioning, in particular its decision-making process, and how the recommendations are made. This knowledge increases the perceived competence users attributed to the system and their trust and acceptance of it. The system transparency appeared to modulate the efficacy of the recommendations and to influence the user experience, for this reason, the authors recommended carefully design the system transparency features.

4.1.2 Actuation

Systems provide personalized support based on the continuous monitoring of specific data from the users’. The way in which the support actions are performed may represent a delicate issue. Putze and Schultz (Putze and Schultz, 2014) focused on adaptive automation task assistance (i.e., Brain Computer Interface system) able to support the operators in situations of high workload. They pointed out that the intrusiveness of the system actions (i.e., usability side effects of supportive adaptive automation) may impact the users' perception of the system’s acceptance and benefits. The balance between the support and the cost of potential discomfort of the user due to the intrusiveness of machine intervention is to be carefully considered (and minimized) to assure the system efficacy. It appeared important that adaptive user interfaces allow users to turn on assisting behaviour only when required.

The timing and modality in which an adaptive system provides recommendations and feedback demonstrated to be a critical issue in the working context. Di Valentin and colleagues (Di Valentin et al., 2015) discussed the usage of on-body sensors to improve ergonomics in the assembly lines. The assistance system is based on the workers' ergonomic potential risks assessment and targeted especially senior employees. The data about the individual’s position ergonomics is collected through haptic sensors and transmitted and visualized graphically in a mobile device. The data served to develop a model of ergonomic health profile, to provide personalized feedback/recommendations for promoting ergonomic-friendly positions and improving the ergonomics of the overall process. In such a way, the system may create an implicit health profile for each worker to improve recommendations regarding the ergonomic bearing. The users' preferences for the development of such ergonomic assistance systems are carefully addressed. In this study emerged that workers expected to receive real-time feedback as soon as they get into an ergonomic unhealthy position. As well, it resulted that the workflow managers preferred to receive overviews of shortcomings in each workflow activity that often lead to unhealthy ergonomic positions and have the possibility to globally analyse the captured data to easily adapt workflows based on those.

In the industrial context, Inagaki (Inagaki, 2003) addressed specifically the issue about the function allocation in human-centered adaptive automation systems, in terms of modulation of the Level of Autonomy (LoA) and decision authority between humans and machines. The paper focused attention on the risks for the human operator of manual skill degradation, vigilance decrements, and loss of situational awareness for the function which may produce a "complacency" situation with high reliable automation. This occurrence may be taken under control through dynamic modulation of LoA, but on the other side of the issue, the author pointed out that the continuous switch between automation and manual control may produce worker performance degradation. Indeed, such situations may determine a reduction in human-machine sharing intention. Moreover, trust in the system may be impacted as a consequence of the "automation surprise" issue. Since adaptive automation behaves in a context-dependent manner through complex and sophisticated algorithms, this behaviour could remain obscure to the users and make them wondering what and why it is acting in that way. The mistrust may cause inappropriate use of automation, and decision authority issues may arise. Indeed, Inagaki observed that users' trust and use of the system may change if its actual system behaviour differs from what they have been anticipated. For this reason, the interface may provide appropriate information to avoid automation surprise effects. Nevertheless, humans may have different feelings or responses when they are overridden by automation, even if for safety reasons. Therefore, the decision authority issue needs a quantitative rigorous (e.g., such as mathematical modelling, computer simulations, and experiments) investigation to be appropriate afforded in the actual context.

Moreover, also in the context of the ubiquitous display environments, Leichtenstern and colleagues (Leichtenstern et al., 2010) reported that the system behaviours impact the fluctuation of the trust levels of the users in the course of his/her interaction with the system (e.g., decreasing whenever an unexpected event occurs). They observed that trust was particularly influenced by the system behaviour transparency and controllability, in addition to the security and privacy policies, and the perceived system's seriousness. In its turn, the perceived system easiness resulted modulated by users' level of trust, thus it should be kept monitored over time.

4.2 Ethic risks

The issues above discussed are closely related also to the ethical dimension of adaptive systems. Indeed, often they are discussed contextually. In this context, the ethics regard the freedom of decision and self-determination principles, and dignity and autonomy of users from one hand, and the socio-economic disparity (Fletcher et al., 2019; Schülke et al., 2010).

4.2.1 Psychological impact

The introduction of the human-robot collaboration paradigm in industrial environments is an example of how the ethical dimension of adaptive systems may impact the users' acceptance of the technology. Fletcher and colleagues (Fletcher et al., 2019) identifies the need for higher consideration and understanding of the ethical and user-centered requirements for the design of such systems to gather their benefits at the production level. To minimize the psychological impact that the robot collaboration may have on the workforce, in terms of both performance and robot trust and acceptance, the authors collected a set of specific design preferences from workers. Behind the requirements related to physical safety aspects of the robot interaction, it appeared the comfort as the most relevant concern of the users. Moreover, the desired design requirements included functions related to the personalization of the machine to the specific needs and preferences of the users. Those preferences disclosed an interest in the psychological concerns and the ethical implications, such as the data monitoring acceptability.

The impact on the operators of the introduction of adaptive systems within the working environment is discussed by Fletcher and Webb (Fletcher and Webb, 2017). The role change due to the escalation of implementation of automation systems able to self-learn and adapt, and perform work for and with humans determine a series of potential ethical and psychological issues surrounding the human-robot collaboration. These concerns are mainly related to the humans' expectation of having a safe interaction both at the physical and psychological levels. The expectations should be calibrated through training and remedial interventions within the organizations. Moreover, the possibility to make informed choices about whether to accept or not the new role change resulted relevant for the workers. Finally, the authors pointed out the importance to address the users' concerns about intrusion related to the inevitable directly or indirectly, overtly or covertly collection and distribution of 'big data' involving also humans adopting appropriate data protection protocols.

Spagnolli and colleagues (Spagnolli et al., 2016) pointed out that humans close relationships with monitoring adaptive machines (i.e., symbiotic systems) may produce asymmetries in values and knowledge whenever one agent gains more benefits or acquire more information than the other. This occurrence might also determine that an agent has more risks than the other. In some specific contexts (e.g., working), this may determine deskilling, and discriminations of users. The ethical issues related to the actions of an adaptive system influence the interaction of the user, having a psychological effect on him/her which may result in usage barriers.

Indeed, in the case of symbiotic systems, a specific discussion emerged from the literature about the ethical aspects related to this interaction. Pacaux-Lemoine & Trentesaux (Pacaux-Lemoine and Trentesaux, 2019) addressed this point. The design of symbiotic systems may incur the risk of machine unethical decisions or "bad habits". Such situations may be derived from the machine underestimation of the process of anticipating situations/experiences, or from the human unawareness of the poorness of the machine learning process. Moreover, the interactive process of learning and decision making may increase the risk of impossible mutual adjustment in hazardous situations/injuries, making the fault responsibility assignment hard. The risk of humans dependence as a consequence of their tendency to progressive functions delegating to the machine, and risk to lose skill and awareness is present, as well the risk of emotional dependence and overconfidence in machine abilities. These risks are depicted by the authors as difficult to eliminate even when an ethical machine design is adopted as they are related to the tight human-machine interaction itself. The implementation of an ethical behaviour framework embedded in the machine program may reduce these risks. This could be made by adopting a deontological paradigm and over-multiplying the number of rules on which the machine can base its behavior. Diversely, it could be made the machines learn from their interactions with humans, or enable machines to evaluate the positive or negative impacts of their decisions regarding ethical criteria and objectives to be reached. The appropriate machine transparency (equilibrated for the number of information users may have without overload) is important to avoid human misunderstanding of current and future machine behavior.

More in general, Trentesaux and Caillaud (Trentesaux and Caillaud, 2020) pointed out some ethical dilemmas which influence the acceptance by the workforce of adaptive systems within Industry 4.0. The ethical stakes they identified are related to the behaviour of intelligent machines and Cyber-Physical Systems and the complexity of this new kind of workplace. They included the risks of disclosing human performance data (whether monitored), the risk of operators' deskilling and errors, the physical and psychological harm risks, and the risk of replacement.

In responding to these issues, authors suggested that: ethical human-machine systems should consider humans' capacities and limits and deal with his/her psychological acceptance while holding the support level of human tasks; ethical cyber-physical systems and robotics should be designed with a unitary design framework with the constraints of satisfaction and use simulation; the AI should be based on deontological and consequentialist ethical models and architectures.

In a previous study, Trentesaux and Rault (Trentesaux and Rault, 2017) focused in the decision-making processes occurring in the Automated Learning Systems, such as the Cyber-Physical Industrial Systems, and the ethical and legal responsibility related, and pointed out the need for a higher consideration of these issues to achieve a human-centred design approach of the Cyber-Physical Industrial Systems.

Trentesaux and Karnousko (Trentesaux and Karnousko, 2020) discussed more in-depth this lack of ethical consideration in Cyber-Physical System design and investigated the reasons for this reluctance and misconception among industrialists and researchers. They observed that it is often derived from an unclear role definition about who is in charge of the ethical knowledge improvement and the rule-based definition of decision-making processes in AI-driven CPS. The spreading belief that the deontological charter would be enough to protect users from unseen situations that may provoke injuries or unpredicted behaviour, or that humans would always be able to regain control over the machine, is commonly adduced as justification. Overall, the authors highlighted that the complexity of the systems, able to self-learn and make their decisions required the implementation of additional practices over the simple safety rules and norms.

The way to consider human values and ethical principles in the context of an augmented industrial environment is the main object of investigation by Longo, Padovano and Umbrello (Longo et al., 2020) in regards to the development of Industry 5.0 (I5.0) in which humans will cooperate with machines symbiotically. The authors reported that human values and ethics could determine a barrier for the evolution towards I5.0 whether they are not considered when implementing the advanced systems. Indeed, their investigations revealed that among industrial employees there is a general agreement on the benefits of augmenting workers' capability, nevertheless, still exist value-oriented and ethical related concerns. First of all, the need to extend the worker's cognitive capabilities is recognized to fill the gap with technology and the capability to interact with other workers and with the cyber-physical production systems intuitively and smartly. Concerns related to the risk that I5.0 technologies cause the loss of jobs whether uncontrolled automation would verify are reported. Another issue was the risk of worker's alienation and depersonalization. Moreover, the possibility of a higher control on working times and duties, with consequent reduced freedom and autonomy for the workers rose. Respondents pointed out the fact that technology should be trustworthy, serve for the common good, and be designed to prevent any possible misuse, and that the digital and automation technology is explicitly considered as a tool that should support accountability and responsibility. Above all, anyway, the need for 'digital trust' is the foremost value for any technology used by humans. The 'honesty', 'explainability', and 'transparency' as well as 'integrity' and 'professionality' has to be pursued likewise. From the point of view of human values, it is observed that the perceived importance for the general values of 'benevolence', 'hedonism', 'power', 'self-direction', 'stimulation' does not change when associated with advanced technologies. While, the importance of 'conformity', 'tradition', 'achievement', 'universalism', and 'security' significantly increases when these values are considered in respect of technology. Especially the 'security' value evaluation revealed as workers (especially the older) strive to get stability and safety in their workplace. Work-related ethical issues such as unethical conduct (e.g., lying, deception, theft), toxic workplace culture, discrimination and harassment, privacy and confidentiality, unethical leadership, unrealistic and conflicting goals, and misuse of technology, are still considered relevant in perspective of I5.0. The value-oriented technology design may be achieved through the workforce's continuous learning and growth thanks to a sharing and collaboration mindset (e.g., knowledge, and expertise) in the context of a 'positive leadership' and a healthy work environment. As well, the ethical design of human-machine symbiosis in Industry 5.0 should consider the 'universality' value. These systems would be fair and respectful of everyone's dignity and opinion equally, not creating relational gaps, but fostering social interactions, preventing worker alienation, and work depersonalization. In this consideration, the authors encouraged the future development of new standards and guidelines alongside the ethical development and use of Industry 5.0 design for human values, suggesting the iterative Value Sensitive Design (VSD) as a suitable approach (Longo et al., 2020).

Villani and colleagues (Villani et al., 2018) considered specifically the societal and ethical implications of advanced automation and collaborative systems aiming to improve operators' performance, enhancing their skills. Vulnerable workers (e.g., elderly, impaired, low-skilled) are especially looked at to attenuate their adverse conditions. This system (namely the affective robotics/computing) operates through self-adaptation based on humans' status. In the paper, it is deeply discussed the impact of such systems on the company organization, in terms of new skills from operators and changes in the organization assets required to face the higher intrinsic complexity of these technologies. The authors proposed a list of recommendations to consider when design and introducing such a system able to measure human capabilities and skills, and adapt themself to those, to train and support the less-skilled operators. These involve the technical aspects the workers need more (e.g., usability and satisfaction), and the ethical (e.g., protecting, non-discriminating for humans), social and legal (e.g., privacy, safety, non-distracting) implications, inspired by roboethics. The major challenges identified by the users in the design of human-machine systems are highlighted. Most of all, the system has to be usable by all users. The information required to interact with the system has to be user-oriented, and human factors should have priority. The main aim of the system has to be the enhancement of the operator's performance, they have to include advanced technological solutions of interaction.

Thekkilakattilet and colleagues (Thekkilakattilet al., 2015) observed a reluctance to develop advances in AI for emerging autonomous intelligent cyber-physical systems as moral agents. Their discussion about the responsibility attribution of failures in Cyber-Physical Systems and Artificial Intelligence systems focused the attention on the management of the decision-making process of these systems. This pointed out the additional need for structuring and demarcating ethical responsibilities among agents (i.e., developers/designers/producers, users, and software) involved in the development and use of intelligent systems. The responsibility should be diverse in function of the machine's decisional capability: namely, automatic machine (i.e., a machine with no decision-making); semiautomatic machine (i.e., a machine with a set of automatic system coordinated by a human involved in the decision-making); semiautonomous machine (i.e., a machine with limited autonomously performing tasks specified by a human); autonomous machine (i.e., a machine capable to decide what and how performing tasks). Such a kind of regulation may favour the acceptance of systems like these among users.

4.2.2 *Societal impact*

The humans' trust in Intelligent Autonomous Systems (IAS) would benefit from the development of moral machines whose design is based on the consideration of public fears and transparency, in addition to the safety standards and regulations. Indeed, the increasing adoption of these systems in various human activities requires carefully consider the impact they could have on society as a whole. Winfield and Jirotka (Winfield and Jirotka, 2018) revealed common ethical concerns related to artificial intelligence, and robotics may impact the population's trust in these technologies. Despite an overall positive attitude towards intelligent technologies, the literature reported specific concerns related mainly to robots: the risk of robot usurpation of human autonomy, safety, and authority. In respect of the world of work, the impact of IAS on jobs and mass unemployment is reported as concerns by the authors. In the author's perspective, the establishment of ethical governance for artificial intelligence and robotics would be a promising way to promote their favourable consideration.

In this regard, Torresen (Torresen, 2018) suggested a reflection on the societal challenges IAS employment is determining. In particular, those related to the job loss due to massive automation (also mentioned in Winfield and Jirotka, 2018), and the risk of human deskilling (also mentioned in Spagnolli et al., 2016) and of AI misuse to achieve destructive and unwanted goals may lead to humankind extinction. Above these dystopian consequences, it emerged as crucial to focus on ethical considerations when developing intelligence systems (namely, moral machines).

To this aim, developers should take care that software aiming to replace human evaluations and social functions should adhere to criteria such as accountability, inspectability, robustness to manipulation, and predictability. The increase in complexity of systems would make this task harder to achieve. Moreover, the ability to make ethical decisions must be improved in intelligent and adaptive systems progressively. Authors, suggested to provide robots with ethical frameworks and internal models to make them self-aware, and thus supporting their ethical behaviour and enhancing safety. Otherwise, developers may also adopt the simulation theory of cognition to enable robots of internal simulations of a set of behavioural alternatives to predict their consequences and make the most convenient decision. Torresen also proposed to afford societal defiances introducing a universal basic income (a sort of "robot tax") and making more efforts to make technology able to provide workers with more leisure time. Additionally, training for humans should be foreseen to improve their interaction capacity. Humans may be able to assure that the technology works effectively and to make their judgments about automatic decision making. As well, the system's design should include mechanisms to prevent human errors and predict the risk of mechanical failure to the extent possible.

The need for particular attention to the societal impact of smart robots is established also by Westerlund (Westerlund 2020 a,b). He evaluated the considerations of the general population of the smart robots, as the increasing adoption of these autonomous systems in various human contexts, and highlighted that the general consideration of this technology is negative concerning their social, economic, environmental impact. In the concluding remarks, the author pointed out the importance of a transparent and universal design for ethical smart robots, as a result of a debate stage on the roboethics.

4.3 Summary

In summary, from the literature analysis highlitghted the existence of a trade-off between the benefits offered by intelligent environments able to adapt and provide personalized services to the users and the users' concerns regarding privacy and personal data protection and ethics. The individuals' perception and beliefs about privacy regulations appeared relevant to the definition of their perception of the risks when interacting with adaptive systems (Lee and Kobsa, 2017; Kobsa and Schreck, 2003; Mannhardt et al., 2019). Weinberg et al. (2015) traced back the main concerns related to IoT to the large amount of users' data collected somehow covertly by these systems. Users' decisions to protect their personal information are highly influenced by their beliefs on the process of data collection and related privacy warrants that might not be realistic (Hamidi et al., 2018). In addition, humans' uncertainty about the reasons for the actual action of the system and the potential future behaviour, may have a psychological impact on users' and influence their interaction with it (Cramer et al., 2008; Leichtenstern et al., 2010; Longo et al., 2020; Winfield and Jirotka, 2018).

Ethical bounds are necessary to limit the actions of such technologies to those respectful of human and societal values. The high complexity of such systems and their increasing capability to make decisions despite humans, determines a huge amount of possible consequences from their behaviour that have to be taken into account, and that are even more increased by the interaction with the human being. Although ethical considerations about adaptive systems open a large inter-disciplinaries debate that appears to be still in its infancy and explorative phases (Trentesaux and Caillaud, 2020; Longo et al., 2020; Westerlund, 2020a,b), a human-centered and value-sensitive design appeared as a promising development towards the achievement of the "moral machine" (Torresen, 2018; Winfield and Jirotka, 2018; Fletcher and Webb, 2017) and the contextual development of adaptive systems regulations and governance (Trentesaux and Rault, 2017; Spagnolli et al., 2016; Inagaki, 2003; Fletcher et al., 2019).

In addition, the system in itself may improve the users' knowledge on these aspects by adopting transparency design features and strategies to explain its functioning to the user (Spagnolli et al., 2018; Spagnolli et al., 2016; Jacucci et al., 2015; Knockaert and De Vos, 2020; Pacaux-Lemoine and Trentesaux, 2019).Training and education practices can further help reduce humans mistakes due to the unawareness (Spagnolli et al., 2016) and worries related to the expected impact of the systems on their life (Torresen, 2018). Especially in working contexts, where the employees' skepticism and fears of being replaced and controlled by machines may represent a relevant barrier to the success of advanced and adaptive automation, interventions directed to the workforce may facilitate the acceptance of the new working paradigm, and highlight the benefits the adaptive systems may bring both to the production and workers (Fletcher and Webb, 2017; Villani et al., 2018).

The main concerns emerged from the literature are the following:

- Filtering (Jacucci 2015; van de Garde–Perik et al., 2006) of the users' data collected implicitly by the machine agent may determine the loss of control and agency by the users over their data.
- Delivery of supporting action/feedback (Putze and Schultz, 2014; Di Valentin et al., 2015) developed on the base of the users' data collected may develop the risk of users' discomfort (e.g., sense of intrusiveness) that may compromise the effectiveness of the support.
- Continuous monitoring (Schülke et al., 2010; Lee and Kobsa, 2017; Putze and Schultz, 2014) by smart devices (e.g., sensors for physiological monitoring) of personal data, especially in the case of data storage in a cloud system leads to the risk of personal discomfort, data usurpation and misused. These latter aspects are particularly considered when users are monitored for health-

related reasons by the devices (e.g., seniors) and the information may determine discriminative effects.

- Communication (Schülke et al., 2010) between multiple smart systems that share information with relevant people for the users may produce concerns about the risk for interpersonal contact replacement, especially in seniors with poor autonomy.

Restricting the focus to concerns especially related to the industrial work environment:

- Human support in working contexts (Longo et al., 2020; Inagaki, 2003; Spagnolli et al., 2016; Pacaux-Lemoine and Trentesaux, 2019; Trentesaux and Caillaud, 2020; Torresen, 2018) through Cyber-Physical Systems and automation may produce in human workers concerns about manual skill degradation, and vigilance decrements. The system interventions may develop worries about the risk of workers' alienation and loss of situational awareness (i.e., complacency with the machine). As well, the worries about the determination of a higher control on working times and duties, and reduced freedom and autonomy may develop.

  In particular, Longo (Longo et al., 2020) discussed the human-value-related risks of three different types of machine support:

  - The focus on perceptual capabilities (e.g., monitoring workers' health and movements via wearable sensors) is related to the risk of compromising the workers' physical and psychological welfare;
  - The focus on interaction capabilities (e.g., intelligent voice digital assistance) is related to the risk of overconfidence in the machine's ability and the exacerbation of potentially harmful humans' behaviours and technical outcomes;
  - The focus on cognitive capabilities (e.g. Simulation-Based VR Training Solutions to Enhance Learning) to promote conformity, minimize impulsive behaviour, and assess the user's improvements over time in terms of compliance with rules and expectations is associated to the risk of easygoing and uncritical adhesion to norms. This in turns decreases the worker's capability to make informed decisions, and leave the worker in unknown situations that are risky for health and safety.

Some guidelines to reduce ethical users' concerns are reported in the next section.

5 Guidelines

n°	GUIDELINE	SOURCE
1	The user should be able to **turn on/off** the assisting behaviour of an adaptive system aiming to provide task support when (s)he needs through the interface.	Putze and Schultz, 2014
2	The adaptive systems should **adapt** gradually, clearly and offer restore options.	Cramer et al., 2008
3	Users should have a way to **correct** a system's adaptive criteria if these appear unsuitable to them.	Cramer et al., 2008
4	**Transparency** features should provide understandable information, limited in the amount of those really necessary and connected to users' goals, priorities, and responsibilities. These features (i.e., explanations) should be embedded in the rest of the interface to counter potential misconceptions in the users.	Spagnolli et al., 2018; Cramer et al., 2008
5	The **interface** design of adaptive systems should make clearly identifiable the adaptive elements to the users.	Cramer et al., 2008
6	The data and information should be provided in an easily comprehensible **language** considering the comprehension skills of the worker.	Villani et al., 2018; Cramer et al., 2008; Longo et al., 2020
7	If natural language recognition is used, the adaptive automation systems should recognize and speak multiple **languages** and accents through advanced Automatic Speech Recognition to reduce discrimination of workers.	Longo et al., 2020
8	The adaptive automation systems should provide visual and textual representation of digital assistant's **utterance** to reduce the discrimination for hearing-impaired workers.	Longo et al., 2020
9	The adaptive automation systems should use culturally-sensitive **terminology** when referring to different categories of workers to reduce discrimination.	Longo et al., 2020
10	The adaptive systems should be used by people with few **computer skills**.	Villani et al., 2018
11	The adaptive systems should be accessible to physically and cognitively **impaired** operators.	Villani et al., 2018

12	The adaptive automation systems' communication mechanisms should avoid overloading the user with **long dialogue** processes.	Inagaki, 2003
13	The adaptive automation systems' communication mechanisms should avoid to **surprise** the user in case of abrupt adaptation based on the users' performance.	Inagaki, 2003
14	The adaptive automation systems employing wearable sensors should use **unobtrusive sensors**, to avoid embarrassed and uncomfortable feelings and sense of intrusiveness, as well to maximize psychological and wearing comfort.	Longo et al., 2020
15	The adaptive systems aiming to preserve the workplace's physical ergonomics should provide workflow managers the **overviews** of shortcomings in each workflow activity that often lead to unhealthy ergonomic positions. The manager should have the possibility to globally analyze the ergonomic data and easily adapt the workflow based on this information through an integrated functionality in the GUI of the WFMS (workflow management systems).	Di Valentin et al., 2015
16	The introduction of adaptive automation systems (i.e., in the form of industrial robots) should include **training** activities for the workforce with comprehensive information about the functionality and reliability of the human-robot system, and about user protocols and risks, to increase trust.	Fletcher and Webb, 2017
17	The adaptive systems aiming to preserve the workplace's physical ergonomics through the development of a health profile should use it to produce ergonomic recommendations **personalized** for each worker.	Di Valentin et al., 2015
18	The adaptive automation systems aiming to preserve the workplace's physical ergonomics should provide workers with real-time **feedback** as soon as they get into an ergonomic unhealthy position.	Di Valentin et al., 2015; Longo et al., 2020
19	The collaborative automation systems should **adapt** (e.g., speed) to correspond with the operator's expertise, skills, capabilities, preferences, and trust level.	Fletcher et al., 2019
20	The collaborative automation systems should adapt to meet varying production demands and **environmental** conditions (e.g. light and noise levels).	Fletcher et al., 2019

21	The introduction of adaptive automation systems (i.e., in the form of industrial robots) should include education of workforce on ethical considerations surrounding protection of individual operators as part of the training and remedial interventions within organizations to support the **operators' change of role** in respect of the new form industrial robot (collaborative) and their acceptance.	Fletcher and Webb, 2017
22	The introduction of adaptive automation systems (i.e., in the form of industrial robots) should include an analysis of the impacts over the workforce of the **work practices change**, considering also the possibility of readjustment of the workforce coping strategies.	Fletcher and Webb, 2017
23	The introduction of innovative systems aiming to enhance workers' capacities can benefit from mechanisms to maximize **social** influencing.	Longo et al., 2020

6 References

1. Albrechtslund, A. (2007). Ethics and technology design. Ethics and information technology, 9(1), 63-72.
2. Belkadi, F., Dhuieb, M. A., Aguado, J. V., Laroche, F., Bernard, A., & Chinesta, F. (2020). Intelligent assistant system as a context-aware decision-making support for the workers of the future. Computers & Industrial Engineering, 139, 105732
3. Benyon, D., & Murray, D. (1993). Adaptive systems: From intelligent tutoring to autonomous agents. Knowledge-Based Systems, 6(4), 197-219.
4. Benyon, D., Innocent, P., & Murray, D. (1987). System adaptivity and the modelling of stereotypes. In Human–Computer Interaction–INTERACT'87 (pp. 245-253). North-Holland.
5. Cohen, Y., Naseraldin, H., Chaudhuri, A., & Pilati, F. (2019). Assembly systems in Industry 4.0 era: a road map to understand Assembly 4.0. The International Journal of Advanced Manufacturing Technology, 1-18.
6. Cramer, H., Evers, V., Ramlal, S., Van Someren, M., Rutledge, L., Stash, N., ... & Wielinga, B. (2008). The effects of transparency on trust in and acceptance of a content-based art recommender. User Modeling and User-adapted interaction, 18(5), 455.
7. Di Valentin, C., Emrich, A., Werth, D., & Loos, P. (2015, December). User-centric workflow ergonomics in industrial environments: concept and architecture of an assistance system. In 2015 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 754-759). IEEE.
8. European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L119 (2016), 1–88.
9. Evjemo, L.D., Gjerstad, T., Grøtli, E.I., Sziebig, G.: Trends in smart manufacturing: Role of humans and industrial robots in smart factories. Current Robotics Reports 1(2), 3541 (2020).
10. Fairclough, S. H. (2009). Fundamentals of physiological computing. Interacting with computers, 21(1-2), 133-145.
11. Felix Putze and Tanja Schultz. 2014. Investigating Intrusiveness of Workload Adaptation. In Proceedings of the 16th International Conference on Multimodal Interaction (ICMI ’14). Association for Computing Machinery, New York, NY, USA, 275–281. DOI:https://doi.org/10.1145/2663204.2663279
12. Fischer, G. (2001). User modeling in human–computer interaction. User modeling and user-adapted interaction, 11(1-2), 65-86.
13. Fletcher, S. R., & Webb, P. (2017). Industrial robot ethics: The challenges of closer human collaboration in future manufacturing systems. In A World with Robots (pp. 159-169). Springer, Cham.
14. Fletcher, S. R., Johnson, T. L., & Larreina, J. (2019). Putting people and robots together in manufacturing: are we ready?. In Robotics and Well-Being (pp. 135-147). Springer, Cham.

15. Gena, C. (2005). Methods and techniques for the evaluation of user-adaptive systems. Knowledge Eng. Review, 20(1), 1-37.
16. Gervasi, R., Mastrogiaconno, L., & Franceschini, F. (2020). A conceptual framework to evaluate human-robot collaboration. INTERNATIONAL JOURNAL OF ADVANCED MANUFACTURING TECHNOLOGY.
17. Hamidi, F., Poneres, K., Massey, A., & Hurst, A. (2018, October). Who Should Have Access to my Pointing Data? Privacy Tradeoffs of Adaptive Assistive Technologies. In Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (pp. 203-216).
18. Inagaki, T. (2003). Adaptive automation: Sharing and trading of control. Handbook of cognitive task design, 8, 147-169.
19. Jacucci, G., Spagnolli, A., Freeman, J., & Gamberini, L. (2015, October). Symbiotic interaction: a critical definition and comparison to other human-computer paradigms. In International Workshop on Symbiotic Interaction (pp. 3-20). Springer, Cham.
20. Klein, G., Woods, D.D., Bradshaw, J.M., Hoffman, R.R., Feltovich, P.J., 2004. Ten challenges for making automation a ‘‘team player” in joint human-agent activity. IEEE Intelligent Systems 19 (6), 91–95.
21. Knockaert, M., & De Vos, N. (2020). Ethical, Legal and Privacy Considerations for Adaptive Systems. In Engineering Data-Driven Adaptive Trust-based e-Assessment Systems (pp. 267-296). Springer, Cham.
22. Kobsa, A., & Schreck, J. (2003). Privacy through pseudonymity in user-adaptive systems. ACM Transactions on Internet Technology (TOIT), 3(2), 149-183.
23. Lee, H., & Kobsa, A. (2017, March). Privacy preference modeling and prediction in a simulated campuswide IoT environment. In 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom) (pp. 276-285). IEEE.
24. Leichtenstern, K., André, E., & Kurdyukova, E. (2010, November). Managing user trust for self-adaptive ubiquitous computing systems. In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (pp. 409-414).
25. Longo, F., Nicoletti, L., & Padovano, A. (2017). Smart operators in industry 4.0: A approach to enhance operators’ capabilities and competencies within the new smart factory context. Computers & Industrial Engineering, 113, 144–159.
26. Longo, F., Padovano, A., & Umbrello, S. (2020). Value-oriented and ethical technology engineering in Industry 5.0: a human-centric perspective for the design of the Factory of the Future. Applied Sciences, 10(12), 4182.
27. Mannhardt, F., Petersen, S. A., & Oliveira, M. F. (2019). A trust and privacy framework for smart manufacturing environments. Journal of Ambient Intelligence and Smart Environments, 11(3), 201-219.
28. OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 23-Sep-1980
29. Pacaux-Lemoine, M. P., & Trentesaux, D. (2019). Ethical risks of human-machine symbiosis in industry 4.0: insights from the human-machine cooperation approach. IFAC-PapersOnLine, 52(19), 19-24.

30. Peruzzini, M., & Pellicciari, M. (2017). A framework to design a human-centred adaptive manufacturing system for aging workers. Advanced Engineering Informatics, 33, 330-349.
31. Preece, J., Sharp, H., & Rogers, Y. (2015). Interaction design: beyond human-computer interaction. John Wiley & Sons.
32. Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In Design automation conference (pp. 731-736). IEEE.
33. Reynolds, C., & Picard, R. W. (2005, July). Evaluation of affective computing systems from a dimensional metaethical position. In First Augmented Cognition International Conference, Las Vegas, NV.
34. Romero, D., Bernus, P., Noran, O., Stahre, J., & Fast-Berglund, Å. (2016, September). The operator 4.0: human cyber-physical systems & adaptive automation towards human-automation symbiosis work systems. In IFIP international conference on advances in production management systems (pp. 677-686). Springer, Cham.
35. Schaub, F. (2018). Context-adaptive privacy mechanisms. In Handbook of Mobile Data Privacy (pp. 337-372). Springer, Cham.
36. Schülke, A. M., Plischke, H., & Kohls, N. B. (2010). Ambient Assistive Technologies (AAT): socio-technology as a powerful tool for facing the inevitable sociodemographic challenges?. Philosophy, Ethics, and Humanities in Medicine, 5(1), 8.
37. Singer, P. (2011) The Expanding Circle Ethics, Evolution, and Moral Progress. Princeton University Press.
38. Spagnolli, A., Conti, M., Guerra, G., Freeman, J., Kirsh, D., & van Wynsberghe, A. (2016, September). Adapting the system to users based on implicit data: ethical risks and possible solutions. In International Workshop on Symbiotic Interaction(pp. 5-22). Springer, Cham.
39. Spagnolli, A., Frank, L. E., Haselager, P., & Kirsh, D. (2018). Transparency as an ethical safeguard. In International Workshop on Symbiotic Interaction (pp. 1-6). Springer, Cham.
40. Thekkilakattil, A., & Dodig-Crnkovic, G. (2015, July). Ethics aspects of embedded and cyber-physical systems. In 2015 IEEE 39th Annual Computer Software and Applications Conference (Vol. 2, pp. 39-44). IEEE.
41. Torresen, J. (2018). A review of future and ethical perspectives of robotics and AI. Frontiers in Robotics and AI, 4, 75.
42. Trentesaux, D., & Caillaud, E. (2020, July). Ethical stakes of Industry 4.0. In 21st IFAC World Congress.
43. Trentesaux, D., & Karnouskos, S. (2020). Ethical Behaviour Aspects of Autonomous Intelligent Cyber-Physical Systems. In International Workshop on Service Orientation in Holonic and Multi-Agent Manufacturing (pp. 55-71). Springer, Cham.
44. Trentesaux, D., & Rault, R. (2017). Designing ethical cyber-physical industrial systems. IFAC-PapersOnLine, 50(1), 14934-14939.
45. Van de Garde-Perik, E., Markopoulos, P., & de Ruyter, B. (2006, October). On the relative importance of privacy guidelines for ambient health care. In

Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles (pp. 377-380).

46. Van De Garde-Perik, E., Markopoulos, P., De Ruyter, B., Eggen, B., & Ijsselsteijn, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. Social Science Computer Review, 26(1), 20-43.
47. Villani, V., Sabattini, L., Czerniak, J. N., Mertens, A., & Fantuzzi, C. (2018). MATE robots simplifying my work: the benefits and socioethical implications. IEEE Robotics & Automation Magazine, 25(1), 37-45.
48. Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. Business Horizons, 58(6), 615-624.
49. Westerlund, M. (2020)a. An Ethical Framework for Smart Robots. Technology Innovation Management Review, 10(1).
50. Westerlund, M. (2020)b. The Ethical Dimensions of Public Opinion on Smart Robots. Technology Innovation Management Review, 10(2).
51. Winfield, A. F., & Jirotka, M. (2018). Ethical governance is essential to building trust in robotics and artificial intelligence systems. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133), 20180085.
52. Wortmann, F., & Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57(3), 221-224.
53. Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. Engineering, 3(5), 616-630.

Appendix 1 - LITERATURE REVIEW TABLE

	Paper (n°/APA)	Type of system	Specific aspect considered	Application Field	Users-related issues	Trust
1	Schülke et al., 2010	Ambient Assistive Technology - Lighting system	USER'S DATA COLLECTION Data cloud	AMBIENT ASSISTIVE LIVING	Monitoring a Ethics	
2	Jacucci et al., 2015	Artificial Intelligence and Symbiotic system	INTERDEPENDENCY HUMAN-MACHINE IMPLICIT USER'S DATA COLLECTION	SYMBIOTIC SYSTEMS	Monitoring a	X
3	Spagnolli et al., 2018	Autonomous / Symbiotic systems	IMPLICIT DATA COLLECTION Enabling transparency to the user.	SYMBIOTIC SYSTEMS	Monitoring b	X
4	Spagnolli et al., 2016	Symbiotic system	USER'S DATA COLLECTION USER PROFILING SYSTEM ACTIONS	SYMBIOTIC SYSTEM	Monitoring Ethics a-b	
5	Pacaux-Lemoine and Trentesaux, 2019	Adaptive Automation	DESIGN OF HUMAN-MACHINE SYMBIOTIC INTERACTION	INDUSTRY 4.0	Monitoring b ethics a	X
6	Fletcher and Webb, 2017	Cyber-Physical Systems - Industrial Robots	OPERATOR'S ROLE CHANGE	INDUSTRY 4.0 HUMAN-ROBOT COLLABORATION	Ethics a	X
7	Hamidi et al., 2018	Adaptive Assistive Technology	DATA COLLECTION	ASSISTIVE TECHNOLOGY	Monitoring b	X
8	Trentesaux and	Autonomous Intelligent Systems	COMPLEXITY	INDUSTRY 4.0	Ethics a	X

	Caillaud, 2020					
9	Trentesaux and Rault, 2017	Cyber-Physical Industrial Systems	MACHINE DECISION-MAKING PROCESSES	INDUSTRY 4.0 MACHINE ETHICS	Ethics a	
10	Trentesaux and Karnousko, 2020	Cyber-Physical Systems	COMPLEXITY	INDUSTRY 4.0 MACHINE ETHICS	Ethics a	X
11	Di Valentin et al., 2015	Ergonomic assistance system	FEEDBACKS AND RECOMMENDATIONS GENERATIONS	INDUSTRIAL WORKPLACE ERGONOMICS	Actuation	
12	Torresen, 2018	Artificial Intelligence and Robots	DECISION MAKING	INTELLIGENT AUTONOMOUS SYSTEMS (IAS) MACHINE ETHICS	Ethics b	
13	Winfield and Jirotka, 2018	Physical robots and Artificial Intelligence	DESIGN	INTELLIGENT AUTONOMOUS SYSTEMS (IAS)	Ethics b	X
14	Villani et al., 2018	Advanced adaptive automation systems - Collaborative robotic	SYSTEM COMPLEXITY	HUMAN-CENTERED INDUSTRIAL AUTOMATION	Ethics a	
15	Fletcher et al., 2019	Collaborative automation and robotics	DESIGN	HUMAN-ROBOT COLLABORATION	Ethics a	X
16	Longo et al., 2020	Cyber-Physical Production System	USER'S DATA COLLECTION DESIGN	INDUSTRY 5.0	Monitoring a Ethics a	X
17,	Westerlund 2020 a,b	Smart robots	DESIGN	SMART ROBOTS	Ethics b	

18						
19	Thekkilakattilet al., 2015	Artificial Intelligence-based Cyber-Physical System	DECISION-MAKING PROCESS Software responsibility (responsibility attribution of system failures)	CYBER-PHYSICAL SYSTEMS	Ethics a	
20	Mannhardt et al., 2019	Sensors data tracking in I4.0 (framework to improve the privacy awareness in the users)	USER'S DATA COLLECTION Users' privacy awareness	INDUSTRY 4.0	Monitoring b	X
21	Knockaert and De Vos, 2020	TeSLA project system for at distance biometric person's identification	USER'S DATA COLLECTION Consent request for the system	AUTHENTICATION AND AUTHORSHIP SYSTEMS	Monitoring b	X
22	Weinberg et al., 2015	IoT-based devices	USER'S DATA COLLECTION	INTERNET OF THINGS	Monitoring a	X
23	Van De Garde-Perik et al., 2008	Personalized recommender service	USER'S DATA COLLECTION	MUSIC RECCOMMENDER APPLICATIONS	Monitoring b	
24	Cramer et al., 2008	User-adaptive art recommender	DECISION-MACKING PROCESS RECOMMENDATION ADHERENCE	ART RECCOMMENDER APPLICATIONS Cultural heritage	Actuation	X
25	Inagaki, 2003	Adaptive automation	FUNCTION ALLOCATION Level of Autonomy modulation	HUMAN-CENTERED AUTOMATION	Actuation	X
26	Kobsa and Schreck, 2003	User-adaptive (or "personalized") applications	USER'S DATA COLLECTION Data anonimization	USER-PERSONALIZED WEB APPLICATIONS	Monitoring system data a	X
27	Putze and Schultz, 2014	Adaptive task assistant - Workload BCI	INTRUSIVENESS	BRAIN COMPUTER	Actuation	

				INTERFACE		
28	Van de Garde-Perik et al., 2006	Health Monitoring System Organization of Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of personal data in context of health monitor systems.	USER'S DATA COLLECTION Relevance of data protection guidelines	AMBIENT INTELLIGENCE	Monitoring b	
29	Leichtenstern et al., 2010	Self-adaptive ubiquitous display environments	TRUST	UBIQUITOUS DISPLAY ENVIRONMENTS	Actuation	X
30	Lee and Kobsa, 2017	IoT devices and services	CONTEXTUAL INFORMATION Perceived Privacy related risks	INTERNET OF THINGS	Monitoring a	