Simona Ghionzoli *

GENERAL SECTION

AI SYSTEMS AT THE WORKPLACE LEGAL TRAJECTORIES BETWEEN PRIVACY AND DRONES 2.0 STRATEGY

Abstract

The case study exam shows that the civil use of drones also concerns production contexts, so talking about drones necessarily implies a reflection on the impact of technology on workers' rights and freedoms.

In fact, it is now recognised that the right to privacy is a principle on which identity and psycho-physical integrity, and therefore individual and collective health and safety, are based.

Firstly, the main national, international and EU regulations that have intervened over time to regulate the matter and that constitute the state of the art will be examined, namely the Chicago Convention of 7 December 1944 on International Civil Aviation, the special provisions made by the Navigation Code, Regulation (EU) No. 1139/2018 unifying the subject matter and the subsequent implementing Regulations No. 945 and 947 of 2019, in an attempt to systematise and understand whether the set of rules currently in force, starting with strict liability, adequately responds to the needs of the commercial development of the sector and to an effective protection of workers.

Market requirements, moreover, require that certain technical standards be met before the product is put into circulation.

Drones, although they have very high levels of automation and can be identified by artificial intelligence systems, according to Art 2 para 2 and Art 6 para 1, are, however, only partially affected by the recent Regulation establishing harmonised standards on artificial intelligence. They are classified as high-risk systems and the Regulation only reserves to them the application of certain provisions concerning product conformity requirements for placing on the market or their use, the first of which is the principle of human oversight. Furthermore, the prerogative of regulatory experimentation spaces (the so-called Sandbox) is provided for in article 57 of the AI Act.

Has an opportunity for the protection of fundamental rights been missed or are the instruments of legal protection, mainly of the psycho-physical integrity of the worker, also linked to the protection of personal data, still guaranteed by Regulation (EU) No. 679/2016 of 27 April 2016?

With this contribution, we intend to demonstrate that the legal institutions contained in the GDPR such as the principle of accountability and in particular privacy by design, DPIA, the tools of negotiation and consultation in the company such as codes of conduct and negotiation with the social partners remain the

* The author is Ph.D (c) in International Studies at l'Orientale University of Naples and Junior Researcher at Re.CEPL, Research Centre of European Private Law, at Suor Orsola Benincasa University of Naples.

DOI 1.13135/2785-7867/11338

most protective and effective for the purposes of implementing the principle of transparency and mitigation of the risks underlying operations that employ pervasive technologies such as drones.
In particular, the unifying Regulation (EU) No. 1139/2018, which shares with the GDPR the legal institution of privacy by design, will be examined.
Having said this, it will be appropriate to examine possible regulatory developments regarding the methods of assessing risk situations to be carried out, if possible, in a shared and preventive manner, right from the development of the software, in order to prepare suitable measures to avert dangerous situations and harmful consequences.
Studying an unprecedented technology such as drones in the context of work is, moreover, both an opportunity and a pretext to reflect on the legal strategies and instruments made available by the legislator to limit and control the exercise of employers' powers.
Mitigating the objective aspects of liability and allocating it in a different way and not only on the operator is another possible development of the legislation.
To the extent that UAVs will be deployed in production contexts, in fact, unprecedented scenarios will open up, which may configure profiles of liability on the part of the employer for the protection of privacy, but will also favour the emergence of unprecedented forms of union bargaining and new organisational models, aimed at strengthening the consent and information of workers as well as improving living and working conditions.

JEL CLASSIFICATION: K15

SUMMARY

1 General remarks[1]

In 1970, with the Statute of Workers' Rights (formerly article 4 of Law No. 300 of 20 May 1970 as amended by Art 23 D Lgs. 151/2015 of 14 September),[2] the Legislator introduced and recognised in the Italian legal system provisions protecting the privacy of workers, which, until then, had only been recognised indirectly and limited to certain

[1] This work is the result of reflections, many of which set out during the scientific internship at Aitronik S.r.l., in S. Giuliano Terme (PI), related to the Ph.D Programme in International Studies. A special thanks to EdgeLab S.p.a. in La Spezia, to l'Orientale University of Naples and to CNR IIT of Pisa for the support in the realisation of this research experience.
[2] Statute of Workers' Rights Art. 4 of Law No. 300 of 20 May 1970 (hereafter Statute of Workers' Rights) as amended by Art 23 par 1 D Lgs 151/2015 on 14 September, so-called Jobs Act (hereafter Jobs Act).

individual aspects, such as those in articles 14, 15, 21 and 2 of the Italian Constitutional Charter.[3]

The latter provision, in particular, absorbs privacy among the fundamental rights of the individual, similarly to what is stated, instead, expressly in articles 7 and 8 of the Charter of Rights of the European Union, signed in Nice on 7 December 2000.[4]

In production contexts, the protection of fundamental rights, first and foremost the right to privacy, is now a central issue, due to the spread and development of increasingly innovative and pervasive technologies, which open up unprecedented video surveillance scenarios.

Regulation (EU) No. 679/2016, reserves an article, namely article 88, entitled "Processing of data in the context of the employment relationship", for the processing of personal data that occurs by means of the use of technology and monitoring systems.[5]

Mobile video surveillance exercised by means of Unmanned Aircraft System, UAS (so-called drones), is used in various operational contexts to ensure first and foremost the safety and surveillance of workplaces, which could not be guaranteed through the use of fixed devices.

The production sectors that have decided to make use of these technologies have mainly been those of logistics and e-commerce for warehouse functions.

It is also worth mentioning the experiences of urban video surveillance in some municipalities, carried out by the municipal police by means of drones (road safety, pedestrian flows, parking times, access to areas closed to traffic, etc) and the surveillance of oil wells, pipeline safety, thermoelectric power stations and industrial plants.

In such areas, artificial intelligence solutions may accompany video surveillance systems, as so-called high-resolution eyes are able to monitor and control areas that are difficult to reach or dangerous and to do so in real time, recognising, through image processing and edge computing and deep learning mechanisms, dangerous situations.[6]

In such contexts, drones use special sensors (thermal imaging cameras, multispectral cameras, etc) to indicate and maintain their flight path and to detect and collect information, carry out surveillance and reconnaissance autonomously. They are equipped with radars, cameras, IR scanners.

Drones process personal data when combined with other technologies and are able to interact with location technology, based on GPS satellites. Integrated technologies could

[3] Domenico Fauceglia, 'Cybersecurity, concorrenza, contratti e cyber-risk' (2020) 1(1) EJPLT 1.
[4] Charter of Fundamental rights of the European Union [2016] OJ EU C 202/389.
[5] Regulation (EU) No. 679/2016 of the European Parliament and of the Council of 27 April 2016 (hereafter GDPR) concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46/EC [2016] OJ L119/1, art 88, par 2, which devolves to the member states the possibility of providing, by law or by means of collective agreements, more specific rules to safeguard the human dignity of the legitimate interests and fundamental rights of the data subjects, in relation to, inter alia, transparency of processing and monitoring systems in the workplace.
[6] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health' (2023) Discussion paper available at <https://www.osha.europa.eu> accessed 05 September 2023.

also include the ability to track devices equipped with Rfid chips and the people/vehicles wearing them. When used with geo-localisation devices, they can intercept communications and electronic devices, leading to the profiling of people.[7]

In fact, they are equipped with 'visual recording equipment' technology with facial recognition capabilities on board or from the ground that allows tracking and identification of persons and sensitive and personal data (see Art 4.1 and 9, para 1, Reg. (EU) No. 679/2016).

Most of them collect information on the daily life of users and their sensitive characteristics including physical and mental states.

Emotion recognition is a highly invasive form of surveillance that involves the mass collection of sensitive and less sensitive and unaccountable personal data, enabling the tracking, monitoring and profiling of individuals often in real time.

They can carry huge amounts of sensors, carry out systematic and penetrating surveillance inside buildings, confirming intrusiveness and potential danger.

In the workplace, one must not overlook the importance of 'movement and location' data as defined by Art 2 (c) of Directive 2002/58/EC as amended by Directive 2009/136/EC,[8] ie "any data processed in an electronic communications network or in an electronic communications service that indicates the geographic location of the user's terminal equipment in a publicly accessible communications service", because they are considered as an identifier, allowing one to identify one's position and trace one's movements and therefore capable of making any subject associated with it identifiable.[9]

This explains the non-existence of anonymous or non-personal location data, because every time the presence of a natural person is identified at a point in space, any information or data will in itself constitute the processing of personal data, which as such needs to be addressed.[10]

Article 4, para 1 of the GDPR mentions, in this respect, 'identifiers' accompanied by the adverb 'any', as elements capable of linking the information to the natural person in order to identify him or her.[11]

[7] Direzione Generale Per le Politiche interne, Dipartimento di Politica Diritti dei Cittadini e Affari Costituzionali, 'Privacy and Data Protection implications of the civil use of drones' (2015), available at <www.europarl.europa.eu/studies> accessed 4 November 2024.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] GU L201/37 consolidated version [2009] GU L337/11.

[9] Giovanni Maria Riccio, Guido Scorza, Ernesto Belisario (eds), *GDPR e normativa privacy. Commentario* (2nd Edition, Wolters Kluwer Press 2022) 790.

[10] Gianclaudio Malgieri, 'La titolarità dei dati trattati per mezzo dei droni tra privacy e proprietà intellettuale' in Erica Palmerini Maria Angela Biasiotti Giuseppe Francesco Aiello (eds), *Diritto dei droni: regole, questioni e prassi* (Giuffré Francis Lefebvre Press 2018) 194.

[11] For an in-depth discussion of the effectiveness of anonymisation and pseudo-anonymisation of personal data see GPDP Provv. n. 5, of 11 January 2024 available at <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977020> accessed 08 March 2024.

1.1 Definitions and categories in national, international and EU legislation

Drones are legally defined as aircraft.

The 1944 Chicago Convention on International Civil Aviation referred in its article 8 to "aircraft capable of being flown without a pilot".[12] The Riga Declaration on Drones of 06/03/2015, states that "drones need to be treated as a new type of aircraft with proportionate rules based on the risk of each operation".[13]

Regulation (EU) No. 1139/2018 in Art 3, para 30, covers "unmanned aircraft" that "means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board".

In order to correctly define and classify aircraft, reference should be made to article 2 of Regulation (EU) No. 947/2019, which contains the definition of UAS or Unmanned Aircraft System, unmanned aircraft and its remote-control devices. UAS means "an unmanned aircraft and the equipment to control it".

This definition is the one preferred by the ICAO (International Civil Aviation Organization). It is inclusive of the aircraft, but also of the network and personnel equipment required to control the aircraft. It differs from the acronym UAV or Unmanned Aircraft Vehicle, which is generically understood as an aircraft designed to operate without a pilot on board, carrying no passengers, remotely piloted, capable of autonomous flight, without reference to equipment.

The regulatory framework on drones consists of a number of acts, which are coordinated in a hierarchical manner with an international level, an EU level and a national level, the latter of which can be traced back to special laws and articulated as follows:

Convention on International Civil Aviation signed in Chicago on 07/12/1944;

Regulation (EU) No. 1139/2018 of 04/07/2018;[14]

Delegated Regulation (EU) No. 945/2019 of 12/03/2019;[15]

[12] Chicago Convention on International Civil Aviation of 07 December 1944 approved and made enforceable by Legislative Decree No. 616 of 06 March 1948 (hereinafter Chicago Convention).

[13] Risoluzione del Parlamento Europeo del 29 ottobre 2015 sull'uso sicuro dei sistemi aerei a pilotaggio remoto (Rpas) noti comunemente come veicoli aerei senza equipaggio (UAV - Unmanned aerial vehicles) nel settore dell'aviazione civile. [2017] GU C355 /09.

[14] Regulation (EU) No. 1139/2018 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1), in so far as the design, production and placing on the market of aircrafts referred to in points (a) and (b) of Article 2(1) thereof, where it concerns unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, are concerned [2018] OJ L212/1, consolidated version [2021] C/2021/2102, corrected on 04 May [2023] OJ L116/30 (hereinafter Reg. (EU) No. 1139/2018).

[15] Regulation (EU) No. 945/2019 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems [2019] L152/1, consolidated version [2020] 09 August L/232 (hereinafter Reg. (EU) No. 2019/945).

Implementing Regulation (EU) No. 947/2019 of 24/05/2019;[16]

Navigation Code (Royal Decree No. 327 of 30/03/1942);[17]

Reg. ENAC UAS IT of 04/01/2021 (for aspects falling under the provisions of Art 2, para 3 of Reg. (EU) No. 1139/2018 and for aspects falling within the competence of the member states).

In the Implementing Regulation (EU) No. 947/2019 of 24 May 2019 on operating rules and procedures for the operation of unmanned aircraft, in force since 31.12.2020, in Art 3, operations are divided into three categories, based on risk. This classification originates from the previous Regulation (EU) No. 1139/2018 of 04 July 2018. This article defines and divides transactions into three categories, namely 'open', 'specific', and 'certified'.

The following UAS can be found in the Open category:

C0 to C4 marked with class identification label;

Unlabelled or marketed before 31/12/2023;

Self-built (for personal use);

With a maximum take-off weight not exceeding 25 kg;

Compliant with the technical requirements set out in Regulation (EU) 2019/945.

For such devices, the operator's registration on d-flight, the pilot's certificate is required, with the exclusion of means weighing less than 25 kg and the obligation of insurance coverage. The maximum flight height is 120 meters and they are required to fly by visual line of sight (Vlos), ie they must maintain a line of sight between the drone and the remote pilot, with a ban on flying over gatherings of people and transporting dangerous goods and releasing materials and substances. They are subdivided into further subcategories: A1, A2, A3. For class A1, operator registration is required when the drone is capable of capturing personal data.

The 'specific' category instead refers to:

drone operations that do not fall under the previous Open category;

operations that take place on standard national or Easa-defined scenarios, effective from 01/01/2024;

For this category, registration on D.flight of operators and operational authorisation (ENAC) is required if they fly over non-standard scenarios.

The categories are subdivided into subcategories that are relevant above all for the purposes of pilot training and operator registration, which are always envisaged, with the exception of subcategory A1 open, which is suggested in the first case, compulsory in the second, when the drone is capable of collecting personal data.

[16] Regular update of the AMC and GM to Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft OJ L/152/45, consolidated version of 4 April 2022 L105/3 (hereinafter Reg. (EU) No 2019/947) - Issue 1, Amendment 2 AMC and GM to the Annex to regulation (EU) 2019/947, Amendment 2, available at <https://www.easa.europa.eu> accessed 4 November 2023.

[17] Regio Decreto of 30 March 1942 approving the Navigation Code (Italy) (hereinafter Navigation Code).

The drones that concern the operational contexts that we are going to examine are mainly those that carry out loading operations, in Vlos as in the case of Ikea Variety drones or Amazon warehouses, or surveillance operations of gas installations or 'Variety Ikea' drones or those in use by the police for urban surveillance.

As of 1 January 2024, in order to place a UAS on the European market, a declaration of compliance with Reg. (EU) No. 945/2019 is mandatory.

Any drone placed on the market before 1 January 2024 without a class label is considered a so-called "legacy" drone, ie they may continue to operate in the Open A1 subcategory if they have a maximum take-off mass of less than 250 grams, including payload, or in the A3 subcategory provided they have a maximum take-off mass of less than 25 kg including fuel and payload. Drones that are not classified and placed on the market after 1 January 2024 are prohibited from use in the Open category if they do not meet the above requirements and may only fly in the specific category.

The 'certified' category presents the highest risk and therefore needs more stringent requirements and safety conditions to ensure high levels of safety. Their use requires the certification of the drone and the operator and the authorisation of the remote pilot when the operation takes place on assemblies of people and involves the transport of people, dangerous goods, or when the size of the drone is greater than three metros. This type of drone concerns future development models for mobility and transport called IAM Innovative Air Mobility and UAM International, Regional and Urban Air Mobility.

1.2 State of the art. The march of drones in national, international and EU legislation. Judicial intersections with AI Act

UAS profanely called drones have different types in terms of shape, size and weight.[18]

A review of the literature shows that even though unmanned vehicles have a separate technology from other classes of robots,[19] they are nevertheless part of the broader genus of robotics,[20] consisting generically of articulated arm robots, humanoid and social robots,

[18] Giovanni La Cava, Angelica Marotta, Fabio Martinelli, Andrea Saracino, Antonio la Marra, Endika Gil-Uriarte and Victor Mayoral-Vilches, 'Cybersecurity issues in robotics' (2021) 12 (3) Journal of wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (Jowua) 1, 28.

[19] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health', available at <https://osha.europa.eu> accessed 05 November 2023.

[20] Lara Merla, "Droni, privacy e tutela dei dati personali" (PhD Thesis, Università degli Studi di Torino 2016) 29. The author recalls some authors such as Ronald Leenes and Federica Lucivero who suggest "*Di cogliere l'intento regolativo del diritto nell'ambito della robotica, secondo una quadripartizione. In primo luogo si pensi alla disciplina dei progettisti e costruttori di robot, quali i droni, attuata attraverso la legge, come nel caso degli standard di sicurezza ISO o le norme sulla responsabilità civile e penale per produttori e utenti dei medesimi. In secondo luogo, il richiamo va alla regolazione del comportamento degli utenti e/o operatori dei droni, tramite il design di questi ultimi, vale a dire progettando queste macchine in modo tale che non sia consentito alcun comportamento illecito degli esseri umani. In terzo luogo si può pensare alla disciplina legale degli effetti dei comportamenti robotici per il tramite delle leggi approntate dal legislatore: è il caso ad es. della contrattualistica e della negoziazione a mezzo di agenti software. In quarto luogo, infine, la legge può mirare alla disciplina del comportamento robotico tramite il suo design, ossia immettendo direttamente i dettami della legge nel software dell'agente robotico. In questo caso AI metodi tradizionali*

unmanned vehicles, which are subdivided into land vehicles, Ugvs and other land robots, underwater vehicles (Uuvs) and aerial vehicles (Uavs).[21] What is important, however, is the difference between autonomous vehicles and remotely piloted vehicles, i.e. autonomous aircraft (SAPR) in which there is no human intervention and in which the flight is totally software-driven, and remotely piloted aircraft (or Apr), a category falling under the concept of unmanned aircraft, in which there is a pilot but operates from a remote station.

The ENAC Regulation of 16 July 2015 combined these two types, ie the SAPR in which there is no pilot but a software, including the APR, in which instead there is a pilot, albeit remotely.[22] Both were considered aircraft under the Chicago Convention on International Civil Aviation of 1944, to which article 743 of the Italian Navigation Code refers, which bases the qualification of an aircraft on a man-made constraint.

The destination constraint is that specified in article 743 of the Navigation Code, which in its first paragraph states that "Aircraft means any machine intended for transporting persons or things by air. Also considered aircraft are remotely piloted aerial means, defined as such by special laws, ENAC regulations and for military ones by decrees of the Ministry of Defence".

To all drones, apart from toy drones, ie drones complying with the Toys Directive 2009/48, which are not subject to registration and cannot be assimilated to aircraft (see Art 1, para 4) ENAC Regulation), the 1944 Chicago Convention on International Air Transport therefore applies.

The assimilation took place, based on Regulation (EU) No. 1139/2018 of 04 July 2018, on common rules in the field of civil aviation and aviation security, followed by implementing acts 945 - New European Regulatory Framework - and 947, which transposed

---

di regolamentazione giuridica, sul piano del dover essere kelseniano "se A, allora B", si affianca - o viene sostituita - da l'intento regolativo della legge tramite il design dei ricavati tecnologici: nel nostro caso i droni. Si tratta di una forma di tecno-regolazione giuridica sul piano dell'essere - o degli automatismi normativi - all'insegna del cosiddetto principio della privacy by design"; see also <https://osha.europa.eu> accessed 04 November 2023 on Unmanned aerial vehicles: implications for occupational safety and health, where UAVS are a class of devices including multirotor drones, as well as single-rotor and fixed-wing devices, hybrid versions, and, potentially, alternative propulsion systems. The common characteristic of these devices is that they are all able to move, with or without a load of some type, in the same (work)space inhabited by humans. In a simplistic view, UAVS are robots that can 'fly' and 'From all UAV types, drones are, unquestionably, the fastest growing class (both in sheer numbers and capabilities). Therefore, the term is often used for the full class of UAVS. As of May 2022, the FAA acknowledged 865,000 registered drones in the United States, including commercial and recreational, with an estimated annual increase of approximately 6.4%. In Europe, the annual increase is estimated between 5.3% and 6.3%, with an accelerating trend (from data available in Molina & Oña, 2017). In both markets, military applications represent the biggest value'; see also Guido Noto La Diega, Machine rules of drones. Robots, and the info-capitalist Society [2016] 2 ILJ 367, according to which (.) indeed, most considerations apply equally to robots and drones, moving from the unrefined, albeit practical, observation that the latter are robots equipped with wings.

[21] Cecilia Severoni, 'Il regime di responsabilità per l'esercizio dei mezzi a pilotaggio remoto', in Erica Palmerini Maria Angela Biasiotti Giuseppe Francesco Aiello (eds), *Diritto dei droni: regole, questioni e prassi* (Giuffré Francis Lefebvre Press 2018) 81.

[22] ENAC Regulation on remotely piloted aircraft of 17 July 2015, available at <www.enac.gov.it> accessed 10 September 2023.

the qualification of UAS, referred to in Art 2 Regulation (EU) No° 947/2019, replacing that of SAPR, in use until then in the legislation.

Regulation (EU) No. 1139/2018, which lays down common rules in the field of civil aviation, certainly also applicable to unmanned drones (see Cons. No. 26), assumed that even drones weighing less than 25 kg were potentially capable of causing harm to persons and property on the surface and, above all, pose a danger to the acquisition and processing of personal data.

It also lays down basic principles to ensure security, privacy and the protection of personal data, through the introduction of basic requirements (Art 55 ff) and a specific bureaucratic procedure to promote technological innovation, which provides for a common certification system.

All types of drones are integrated, regardless of weight and size, within the framework of Easa's Common Aviation Security.

It partly implemented the Riga Convention of 06 March 2015, whereby drones were all to be treated as a new type of aircraft, dictated key points for the future regulation of drones for civil use, including the protection of privacy, equated manned drones with unmanned drones, stipulated that safety rules were to be commensurate with the actual risk of each individual operation, which it is easy to see how it presents problems, especially in terms of privacy and security of data and networks.[23]

Under the pretext of privacy, the criterion of weight was overcome and additional elements emerged, for the purposes of the configuration of liability, such as the risks associated with the activity, such as that relating to the processing of personal data.

The recent measures of the EU legislator, such as the AI Act and the Cyber Resilience Act, proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) No. 1020/2019 (see Art 2, para 3), the former merely amends and supplements Regulation (EU) No. 1139/2018, and the latter excludes from its scope products with digital elements that have been certified in accordance with Regulation (EU) No. 1139/2018, which are drones, as they are treated in the same way as products with digital elements, in particular those for civil use, and those developed for exclusively military or national security purposes are also completely excluded from the regulatory scope.

The Regulation of the European Parliament and of the Council, which establishes a common framework of rules on AI, in Art 2, in the first version, stated “For AI systems

[23] Theresa Papademetrio, ‘Regulation of Drones: European Union’ (Report April 2016 USA, the Law Library of Congress, Global Legal Research Directorate), available at <http://www.law.gov> accessed 30 September 2022; the author outlines the key guiding principles to be considered in the future regulation of drones whereby Drones must be treated as a new type of aircraft and any safety rules imposed must be proportionate to the risk of each operation. It is crucial that the EU immediately establishes safety rules and standard technologies for the integration of drones into civil aviation. It notes how protecting people's privacy will lead to greater public acceptance. It reiterates that the operator of a drone is responsible for its use and in relation to this last principle the Declaration raised the issue of liability and insurance aspects.

classified as high-risk AI systems in accordance with Articles 6, para 1 and 6, para 2, related to products covered by Union harmonisation legislation listed in annex II, section B only article 84 of this Regulation shall apply. Article 53 shall apply only insofar as the requirements for high-risk AI systems under this Regulation have been integrated under that Union harmonisation legislation". Well, drones were included in Annex II, section B, and consequently, the Artificial Intelligence Regulation would apply to them, but only limited to certain provisions.

In the current version of the Regulation approved on 13 June 2024, article 2, para 2, refers to article 6, para 1, and classifies drones as high-risk artificial intelligence systems and confirms that only articles 102 to 109, article 112 and article 57, which govern sandboxes, are applicable to them, limited to cases in which the requirements for high-risk artificial intelligence systems, pursuant to the regulation, have been incorporated into union harmonisation legislation (see Art 108 AI Act, which calls for the requirements set out in chapter III section 2 AI Act to be taken into account).

According to Art 6, para 1, AI system is considered to be high-risk if two requirements are fulfilled, ie if it is intended to be used as a safety component of a product or is itself a product covered by the Union harmonisation legislation listed in annex I, and at the same time the product, the safety component of which within the meaning of (a) is the AI system or the AI system itself as a product, is subject to a third-party conformity assessment for the purpose of placing that product on the market or putting it into service again under the legislation listed in annex I, traceable to Regulation (EU) No. 1139/2018.

AI Act has a product-oriented approach.[24] This regulation shares with the GDPR and Regulation (EU) No. 1139/2018 the concept of privacy and security by design, certification mechanisms, risk assessment and measurement, and mitigation tools.

Furthermore, with the adoption of the Cyber Resilience Act, certain regulatory gaps will be resolved and consequently cybersecurity, too, will be considered a priority element in design, the lack of which may constitute a defect in the product.[25]

Recognition of the product's lack of security, also due to the lack of defence mechanisms against cyber-attacks, could reasonably lead to the assumption of a case of liability by omission.[26]

Statistics show, in fact, accidents to persons and acts of hacking, mainly involving drones flying over long distances (Bvlos).[27]

These are cyber-physical systems and therefore exposed to cybercrime more than other devices. The most exposed are precisely those for recreational or commercial use, which

[24] This feature of the AI Act also emerged at a conference, organised by the Cesifin Foundation 'Persona, dati personali, algoritmi, tra GDPR e AI Act' (17 June 2024 Florence). See speech by Professor Salvatore Orlando "Decisioni algoritmiche, diritto di spiegazione e tutela dei consumatori".
[25] Giovanna Capilli, 'I criteri di interpretazione delle responsabilità' in Guido Alpa (eds), *Diritto e Intelligenza artificiale* (Pacini Press 2020) 485.
[26] ibid.
[27] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health' (2023), available at <https://osha.europa.eu> accessed 05 November 2023.

are more vulnerable to hacker attacks because they are equipped with less sophisticated systems.

The danger therefore exists not only for privacy, but also extends to the security and protection of personal data.

Indeed, drones collect information and transmit it and can be connected to the internet, introducing the Internet of Drones (IOD) theme, are products that also consist of a software component that is often connected to or involves the cloud.[28]

Assuming proactive behaviour subsumed under the concept of privacy and security by design and, above all, anticipating threats is very important for designing software and averting possible external attacks or internal incidents, with inevitable liability profiles[29] and significant psycho-social impacts in the workplace.[30]

2 Drones at workplace. Case studies

The European Agency for Safety and Health at work conducted a study, called 'Drones inspecting worksites of gas infrastructure operators (ID 16)', from which it emerges that an increasing number of companies are using artificial intelligence or advanced robotics in work contexts, for reasons related to the efficient organisation of production and to ensure, also, greater worker safety, with the aim of reducing boring, repetitive and dangerous tasks.[31] These objectives, however, must be reconciled with the need to protect their fundamental rights, first and foremost that of privacy and data protection.

The case studies examined concern the use of drones to inspect work sites of gas infrastructure operators by means of drones and a visual system based on artificial intelligence, drones for efficient warehouse logistics, drones for surveillance of urban areas.

Drones for pipeline surveillance: In Norway there are interesting experiences with the use of drones for the maintenance and surveillance of gas infrastructures, located above ground and exposed to the weather. The use of drones, supported by artificial intelligence systems, is useful to minimise risks for workers, who have to move over different altitudes. Drones fly over very large areas to supervise sites and simplify maintenance.

[28] Domenico Raguseo, Rosita Galiandro, Giuseppe Marullo and Antonio De Chirico, 'Cybersecurity for Drones. Types of attacks', available at <www.ictsecuritymagazine.com> accessed 10 November 2023.
[29] G Alpa, *Manuale di diritto privato* (Wolters Kluwer Press 2020) 916. The author, while critical of such a jurisprudential approach, nevertheless reports that the assumption that "*La colpa per omissione ha quale presupposto l'esistenza di un obbligo di agire per evitare l'altrui danno o per rimuovere una situazione di pericolo dove l'individuazione del presupposto dell'illecito non riguarda soltanto la prevenzione di un fatto dannoso, ma anche quella di un fatto potenzialmente dannoso e non ancora attuale: di qui l'ammissione dell'esistenza di un "illecito di pericolo" da molti ignorato nelle elaborazioni dottrinali che proprio in materia di colpa omissiva manifesta i suoi aspetti essenziali*".
[30] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health' (2023), available at <https://osha.europa.eu> accessed 05 November 2023.
[31] European Agency for Safety and Health at Work, 'Drones inspecting worksites of gas infrastructure (ID 16)' (2023), available at <http://osha.europa.eu> accessed 15 September 2023.

The drones are supported by cameras and algorithms, searching for specific obstacles and dangers. The algorithm, pre-trained on a large database of indexed images, analyses the visual input of the camera specifically for fallen or forgotten objects on the ground, classifying the objects to be removed and informing the operator.

Through the quality of the image, a reliable result is guaranteed. The quality originates from the algorithms.

The visual inspection system is based on artificial intelligence-based back-end software, which performs a cognitive and informational task.

The analysis of the images is based on information, which leaves little or no room for human evaluation activities, which are limited to carrying out what comes out of the drone's analysis (recovery and removal of fallen objects, minor and major repair work).

The use of these devices contributes significantly to improving safety in the workplace and is also relevant at the psycho-social level, because it fosters the acceptance of digital innovation in the company, linked to the perception of the usefulness of these tools and interaction with them through the preparation and participation in appropriate training plans.[32] This will contribute to the enhancement of skills, self-esteem and trust in the company. There will also be benefits for the improvement of the climate and inter-human relations in the company, linked to the increase in time available for sharing and confrontation, taken away from production.

Space and working time will be progressively enhanced and made more efficient. This will correspond to an increase in the quality of life in the workplace especially if it is accompanied by a reconsideration of working time and working hours through bargaining.[33]

Verity drones: Ikea is the first retailer to use Verity for night-time inventory checks, ensuring product availability online and in shop.

Drones help improve inventory accuracy, increase productivity, lower labour costs for warehouse management, and increase efficiency and employee satisfaction. They are able to detect an error before it can turn into a system flaw. By means of drones, work automation systems are introduced, which although they may be repetitive, are characterised by dynamic elements such as the ability to analyse work processes.

Warehouse operators are able to detect errors in advance, ie before the pallet is picked, using images captured by drones. The inventory manager examines the report in the verity cloud before the start of the first shift, identifying errors to be corrected together with the workers, who are involved from the beginning in the analysis, correction of malfunctions and updates. Repetitive and boring tasks such as frequent cycle counts are significantly reduced. The drones are released at night and are supplemented by

[32] Tiziano Treu, 'La digitalizzazione del lavoro: proposte europee e piste di ricerca' (2022) 32 (1) Diritto delle Relazioni Industriali 17.
[33] Anna M Ponzellini, 'Tecnologie, fine della presenza e dilemmi del controllo nei nuovi pattern spazio-temporali del lavoro' (2020) 1 Economia & Lavoro 89 ff.

thermal infrared night vision sensors. They scan the pallets moved in the last 24 hours and the data collected is used to correct errors and provide feedback to workers to facilitate training and process improvement.

The implementation of automation processes in the company, by means of surveillance and AI systems, in this case increases motivation in employees and speeds up production processes, contributes to a greater involvement of the former in the production processes and gives responsibility to supervisors, who are called upon to take note of errors and resolve them.[34]

Drones for surveillance of urban areas: they are used for investigation activities, environmental and building police tasks, surveillance of public buildings or buildings of public interest, traffic accident detection and traffic monitoring, safety and security operations at public events, civil protection activities, prevention and fight against drug offences, rescue and search of missing persons in hard-to-reach areas.

During such operations, it is very easy to violate the privacy of both the workers who use the device and the people who happen to be filmed.

Many Italian municipalities have provided for the use of drones in their Municipal Police Regulations and in order to do so, some preparatory activities, inherent to the implementation of the principle of accountability, have been necessary.

They consist in the preparation of appropriate documentation for the data collection and processing activities, including the security measures adopted to protect personal data from the outset, the first of which is the pact for the implementation of urban security, signed by the Mayor and the Prefect (see Decreto Legge No. 14/2017, Art 5, para 2) (a), of 20 February 2017).[35]

The aforementioned plan outlines the path required to be in line with the GDPR and other sector regulations and to increase accountability, which starts with a description of the starting state of the organisation's video surveillance systems and its IT systems and ends with their compliance and the pursuit of certain objectives.

In this architecture, an important component is confirmed to be that relating to the performance of the DPIA to calculate the risk associated with processing, the purposes of which have already been defined and must be in line with the principles of Art 5 in conjunction with Art 24, which contains the principle of accountability, ie the implementation by the data controller of all technical and organisational measures to ensure and demonstrate that processing is carried out in accordance with the GDPR regulation, right from the early design stages.[36]

[34] Verity, 'Maximizing value. Client success stories in harnessing Verity's benefits' (2023), available at <http://verity.net> accessed 15 April 2023.
[35] For an in-depth examination see GPDP, Provv. No. 234, of 11 April 2024, available at <https://www.garanteprivacy.it> accessed May 2024.
[36] Luca Bolognini and Enrico Pelino (eds), *Codice della disciplina privacy* (Giuffré Francis Lefebvre Press 2019) 201.

Article 35 GDPR is compulsory when the processing involves, in particular, the use of new technologies, which entail risks for the rights and freedoms of persons (see Art 35 para 1) and must take place before the specifications for the purchase of hardware and software tools are prepared.[37]

DPIA is one of the most important declinations of the accountability principle, because it takes place before the treatment itself and also concerns the type of instruments that will be used.

The DPIA provides for the optional consultation of data subjects or their representatives (see Art 35, para 9), which confirms its meaning as an in advance risk assessment tool.

The risks refer to the rights and freedoms of data subjects (see Art 35, para 7, (c), Cons 90 for sources of risk and Cons 84) and relate to the assessment and management of processing risks in both the IT and organisational spheres. The DPIA must be carried out in respect of each of the elements described in article 35, para 7, in relation to each processing operation/tool used. Among these, data protection (also of employees) is very important.

In all three cases considered, the DPIA is necessary, due to the innovative use or application of new technological or organisational solutions as referred to in Art 35, para 1, Reg. (EU) No. 679/2016, as well as due to the presence of at least two of the prerequisites set out in the list in WP 29 consisting in the large-scale systematic monitoring of publicly accessible areas and in the processing of personal data of the operator and/or employees (eg log files or navigation data tracked for security reasons), using the devices to perform work in the case of drones for plant surveillance and in the warehouse, which may give rise to predictive analysis and thus to automated processing, including profiling.[38]

2.1 Drones and employer control powers between GDPR and the Workers' Rights Statute, as amended by the Jobs Act

Legislative Decree No. 151/2015 (Cd. Jobs act), Art 23, as known, treated the matter of remote controls, in an opposite way to the discipline of Law No. 300/1970 (so-called Statuto dei Lavoratori), ie it abrogated the general ban on the use of equipment for the purpose of remote control of workers and revised the discipline, recognising the possibility of their use in typified cases (organisational and productive needs work safety and protection of company assets) and provided that they are accompanied by the stipulation of trade union agreements.

[37] See Cons. 75 and 78, as well as Art 35 par 3 GDPR and the Guidelines WP 248 rev. 01, GDPD, Provv. No. 467, of 11 October 2018, available at <https://www.garanteprivacy.it> accessed 10 January 2019 and at <https://www.ec.europa.eu> accessed 11 January 2024.

[38] See also GPDP Provv. No. 5, of 11 January 2024, available at <https://www.garanteprivacy.it> accessed 10 March 2024.

Moreover, the legislator, taking into account the changes due to technological evolution, has made certain devices indispensable for work performance and has provided for specific rules for them, exempting them from the obligations set out in Art 4, para 1, preferring to intervene on the limits to the use of the data collected through them rather than prohibiting them.

The vagueness of the expression "working tools", which does not find a precise match on a semantic and regulatory level, gives way for the interpreter and opens up the configuration of different orientations. The first that brings back to the notion of work tools the individual devices assigned to the worker for organisational needs and directly used by the latter not only for the performance of work, but also to make it efficient[39], considering, on the contrary, to be excluded all the others, such as the device or the software program application, when they are not functional to this and instead have exclusive control purposes. According to the orientation set out above, what matters for the purposes of qualification and classification seems to be the usefulness of the device and its components to render the service, to be assessed taking into account the production and organisational requirements, so as to ensure the exact performance of the work service, deduced in the contract. The second, according to which the software allows the operation of the former, but also allows the massive storage of the data in transit of the workers (becoming instruments of remote control), consequently they may be considered instruments of work and fall within the facilitated regime under para 2, only on condition that they are coessential and indispensable for rendering the work performance, considering, on the contrary, that the exception regime must be excluded in the event the performance can nevertheless be rendered even without the aforesaid instrument.[40]

The latter orientation is confirmed by Art 15 of Recommendation CM/Rec (2015) 5 of 1 April 2015, of the Committee of Ministers to Member States on the processing of personal data in the employment context, which reiterates the necessary participation of trade unions in the employer's choices regarding the installation and use of electronic control and surveillance devices (in whatever form this takes place), which remain the ultimate hypothesis to be taken into consideration for the achievement of certain objectives of an organisational nature.[41]

In general, any technical device, including but not limited to the use of video-surveillance systems, which may result in the processing of personal data or which is even

[39] See Carlo Pisani, 'Gli strumenti utilizzati per rendere la prestazione lavorativa e quelli di registrazione degli accessi e delle presenze' in Carlo Pisani, Giampiero Proia and Adriana Topo (eds), *Privacy e lavoro la circolazione dei dati personali e i controlli nel rapporto di lavoro* (Giuffré Francis Lefebvre Press 2022) 445 ff; in jurisprudence see the recent decision of Cass. Civ., 03 June 2024, No. 15391, available at <https://www.dirittoegiustizia.it> accessed 8 June 2024, whereby if installed on company cars intended for the performance of specific services, the telepass must be considered a tool directly functional to the efficiency of the individual performance, as well as now strongly interpenetrated with it in today's working practice.

[40] See Riccio, Scorza and Belisario (n 9) 914.

[41] See CM/Rec (2015) 5, of 01 April 2015, available at <https://www.garanteprivacy.it> accessed 5 November 2024.

potentially capable of doing so, because it collects and processes employee information capable of identifying them or of making them identifiable (see Art 4, para 1, and Art 2 of the GDPR), is liable to result in direct and indirect control.[42]

Drones, although high-precision instruments, when equipped with cameras or sensors, theoretically allow the recording of movements and are able to capture images from the ground with a high level of precision, due to their discretion and versatility. The zoom makes it easy to track people. This means that from work tools[43] that can be used, among other things, for the defence of property, but also of health and psycho-physical integrity, they can be transformed into tools for control of work performance. Directly because of the use of surveillance technology (zoom, video cameras, sensors, etc.), indirectly because of the collection, detection, storage, processing and examination of data and the potential use that can be made of them, for the purposes of predictive, evaluative analyses, profiling of habits and behaviour.

Their use, in the above-mentioned cases, could lead to the transition from a mere presence detector to a remote-control tool[44] due to the collection and processing of data that takes place over a prolonged and continuous period of time; from this point of view, it can only take place after verifying the need to reach a collective agreement with the workers' representatives, pursuant to Art 4, para1, of the Workers' Rights Statute.

Article 88 on the "processing of data in the context of employment relations" devolves to the member states the possibility, through laws and collective agreements, to provide for rules that are more specific to guarantee the protection of rights and freedoms, with reference to the processing of employees' personal data in the context of employment relations and in the second paragraph also specifies how, ie guaranteeing and regulating the transparency of the processing, the transfer of personal data within a group of companies, or a group of companies carrying out a common economic activity and workplace monitoring systems.

Article 88 GDPR speaks of data processing in an all-encompassing way and referring to all workplace monitoring systems, not just video surveillance.

---

[42] *Soc. Italcementi Vs. Fillea CGIL* [1986] No. 1490 Cass Civ available at Arch Civ 1986 155 sofor which what is relevant is the installation of the system, from which remote control of the workers may result, despite the absence of activation of the same, which is such as to require the consent of the trade union or the labour inspectorate, the only ones able to assess the suitability of the instruments to harm the dignity of the workers and the actual compliance of the same with the technical production requirements also with reference to an instrument other than video surveillance; see also Cass. Pen. [2019] No. 50919, available at <https://Foroplus.it> accessed 5 May 2024 for which the violation of the guarantee procedure under Article 4, protecting interests of a collective and super-individual nature, is used to assess the suitability of the instrument to injure the dignity of workers and the effective compliance of the same with the technical production and safety requirements. In the same sense see Cass. Pen. [2014] no. 4331 for which "*c'è violation dell'Art. 4.1 n. 300/1970 anche se l'impianto non è messo in funzione: poiché il bene giuridico protetto è la riservatezza dei lavoratori e il reato in questione si configura come un reato di pericolo, la norma sanziona a priori l'installazione, prescindendo dal suo utilizzo o meno*", mentioned in Bolognini and Pelino (n. 36) 1385.

[43] Giulio Donzelli, 'L'interazione uomo macchina tra tecnologie digitali e successo industriale' in Guido Alpa (eds), *Diritto e Intelligenza artificiale* (Pacini Press 2020) 98.

[44] Cass.Civ. [2016] available at Just Civ Mass, 2016, mentioned in Giulio Donzelli (ibid); on this point see also Council of Europe Recommendation of 1 April 2015 CM/Rec (2015) 5 prohibiting prolonged, constant and indiscriminate controls, available at <https://www.garanteprivacy.it> accessed on 20 May 2020.

The processing of personal data carried out within the framework of the employment relationship, if necessary for the purposes of managing the relationship (see Art 6, para 1 (b) and (c) and Art 9, para 2 (b)) must, however, be carried out in compliance with the principles set out in Art 5 of the Regulation and in particular with the principle of lawfulness, according to which processing is lawful only if it complies with the applicable sectoral regulations (see Art 5, para 1 (a)).

The prerequisites of lawfulness brought by the specific regulations and guarantees of the sector, are those set out in article 4 of Law no. 300 of 20 May 1970, to which articles 113 and 114 of the Privacy Code refer, which are regulations bearing greater and more specific guarantees than those considered by article 88 GDPR.[45]

Article 4, para 1, of the Statute, as amended by Legislative Decree No. 151 of 14 September 2015, peremptorily identifies the cases in which video-surveillance instruments may be used in the workplace and if they give rise to the possibility or danger of remote monitoring of workers, precise procedural guarantees are established.

The case of drones could fall within this case, as there is also only the danger of remote control or profiling and predictive automated processing (in the event of data retention beyond a certain period of time).

Article 4, para 2, introduces an exception to the restrictive regime just considered in the case of instruments used to record presence on duty and to render work performance.

Access to the facilitated regime, at the centre of the doctrinal debate already examined, was recently the subject of a provision of the Privacy Authority, which resolved a similar case on the basis of the criterion of the retention time of e-mail logs, which may not exceed 21 days; otherwise they could be suitable to entail an indirect remote control of workers and therefore be framed under para 1 of Art 4 of the Statute, in so far as they are also potentially capable of collecting information relating to the personal sphere or opinions of the person concerned and therefore not relevant to the performance of the work.

Finally, Art 4, para3, introduces also further profiles of unlawfulness when there is further use of the personal data collected. According to para 3) of Art 4 of the Statute as amended by Art 23 Legislative Decree 151/2015, “the information collected pursuant to paragraphs 1 and 2 may be used for all purposes connected with the employment relationship provided that the employee is given adequate information on the manner of use of the instruments and of carrying out the checks and in compliance with the provisions of Legislative Decree no. 196 of 30 June 2003.

The processing of data in these cases must also be accompanied by an appropriate level of fairness and transparency towards the employees, who must have been adequately informed (see Art 5, para 1 (a) and arts 12, 13, 14 GDPR). To this end, in addition to following the indications contained in the provision on video surveillance of the Privacy

[45] See GPDP, Provv. No. 364, of 06 June 2024, available at <https://www.garanteprivacy.it> accessed 10 June 2024.

Authority of 08 April 2010, No. 1712680, it is also necessary to bear in mind the Guidelines No. 3/2019 of the European Data Protection Committee on the processing of personal data by means of video devices.

According to the latter, in the case of video-surveillance systems, the first-level information notice, by means of appropriate signs in the vicinity of the area concerned (purpose, data controller, data subject's rights, data retention times, data processing methods, etc.), must be accompanied by a second-level information notice, to which the first will expressly refer, so as to provide data subjects with the means of consulting the information notice in full and all the other elements indicated in Art 13 of the Regulation.[46]

The reference is therefore directed not only to the GDPR rules but also to the applicable sectoral regulations (see Art 5, para 1, (a)), so as to ensure a fair balance between the interests of the data controller and in particular the economic/organisational interests of the employer and the privacy needs of the data subject, so as not to incur abuses and so that processing is in compliance with the principle of fairness and loyalty (Art 5, para 1 (a)) as well as the conditions for the lawful use of technological tools in the work context (Art 88, para 2 GDPR).[47]

Article 88, on the one hand, did not affect the national rules of greater protection (ie the specific rules) aimed at ensuring the protection of the rights and freedoms with regard to the processing of workers' personal data, such as Art 23 of Legislative Decree No. 151/2015 (formerly article 4 of Law No. 300 of 1970), on the other hand, however, it opened up the possibility of delegating to collective agreements (including supplementary ones as it appears from Cons. 155), the regulation beyond and exceeding the distinction in paragraphs 1 and 2, provided that it is more specific and more protective for workers.[48]

The internal legislation, moreover, has been approved as a specific provision Art. 114 of Legislative Decree No. 196 of 30 June 2003, the Privacy Code, which among the conditions for the lawfulness of processing has established compliance with the provisions of Art. 4 of Law No. 300 of 1970, whereby if video surveillance systems can derive even

[46] On this point, there is a conforming orientation of the EDPB and the GPDP, mentioned in Provv. No. 5, of 11 January 2024, available at <https://www.garanteprivacy.it> accessed 10 June 2024 and in case law Cass Civ [2024] No. 15391, available at <https://www.dirittoegiustizia.it> accessed 10 June 2024 whereby "*posto che il telepass installato su iniziativa datoriale sull'autovettura messa a disposizione del dipendente … consente la registrazione del transiti autostradali e che dunque, in questo modo, si può effettuare un controllo a distanza, seppure postumo, tale teorica o concreta possibilità di controllo rende utilizzabili i dati ricavati da tale strumento solo se il lavoratore è stato previamente ed adeguatamente informato delle modalità d'uso dello stesso e dell'effettuazione dei controlli nel rispetto di quanto previsto dalla normativa sulla privacy, come sancito dal comma 3, dell'Art. 4 Legge n. 300/1970*".

[47] Article 88 GDPR par 1 "Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship".

[48] See Silvia Ciucciovino, 'Art. 88 commento' in Roberto D'Orazio, Giusella Finocchiaro, Oreste Pollicino and Federica Resta (eds), *Codice della privacy e data protection* (Giuffré Francis Lefebvre Press 2021) 948 ff.

only from the possibility of remote monitoring of employees they may only be used for purposes related to production and organisation, for the safety of work and the assets of the company. The relevant installation must be carried out subject to a collective agreement with the unitary or company trade union representatives or with the authorisation of the labour inspectorate, constituting a condition without which video surveillance systems cannot be installed, without running the risk of violating Art 171 of the Privacy Code.[49]

Violation of article 88 of the GDPR is, on the other hand, subject to the application of an administrative sanction under Art 83, para 5 (d).

There are, therefore, various and autonomous levels of guarantee, constituted first and foremost by the Privacy Code as well as by article 4 of Law 300/1970 (as amended by article 23 of Legislative Decree No. 151/2015) to which Art 88 refers in conjunction with arts 5 and 6 GDPR. The GDPR extends, however, bargaining with the social partners beyond and notwithstanding the differences contained in the internal regulations and with specific reference to the processing of personal data, which if pertaining to software and technological evolution, inherent in surveillance tools, is capable of favouring the storage and massive processing of data and which may concern, therefore, their use and the purposes of processing or other aspects that will be discussed in more detail below.

The distinction made in Legislative Decree No. 151/2015 allows for the expansion of a guarantor norm, which can open up interesting opportunities for protection and negotiating weapons in the hands of the worker in both the pathological and physiological phases of the employment relationship, where the guaranteed procedures, which are made safe by the GDPR, are not observed.[50]

In 2023, the European Agency for Safety and Health at Work adopted a document entitled “Automating physical tasks using AI-based systems in the workplace. Cases and recommendations”, in which, while emphasising that the use of drones in the workplace is intended to be a supportive tool for workers and for the company, capable of guaranteeing greater privacy for the former compared to traditional full-camera systems, it does not fail to recommend “the full inclusion of workers and managers in all technological implementations”, through trade unions and employers' associations. Any system that processes sensitive data should thus be accompanied, as the Agency writes, at least by Codes of Conduct. The latter, in addition to accompanying the software at the time of design and development, can also serve as guaranteed instruments at a later stage, ie, at the time of installation and use of AI systems.[51]

[49] See the extensive examination in GPDP, Provv. No. 58, of 02 March 2023, available at <https://www.garanteprivacy.it> accessed 5 November 2024.
[50] Ciucciovino (n 48) 950.
[51] European Agency for Safety and Health at Work, ‘Automating physical tasks using AI-based systems in the workplace. Cases and recommendations’ (2023), available at <https://www.osha.europa.eu> accessed 5 November 2024.

There are, in fact, situations in which drones are supplemented by thermal sensors for infrared night vision and are therefore apparently harmless to privacy, as is the case with Ikea's Verity drones, which can also be used in sectors such as agriculture and construction. In the future, these devices will be able to function completely independently and will contribute to the development of systems for the automation of physical and cognitive tasks in the workplace, with considerable impact on workers, privacy and data.

2.2 Drones and worker protections in the GDPR and the AI Act

The adoption of proactive behaviour, subsumed under the concept of diligence pursuant to arts 1218, 1176, 2087 of the Civil Code,[52] and accountability pursuant to article 24 of the GDPR, contribute to the social acceptance of these technological devices by workers, supported by the perception of the real utility and benefits that they are able to bring.[53]

The European Social Partners' Framework Agreement on Digitization of June 2020, between the European Trade Union Confederation (ETUC), Business Europe, SGI Europe and SME United, reaffirms, not incidentally, the centrality of the person at the helm of production processes and emphasises that digital systems must comply with existing law, but also with the GDPR, so as to make use of all the tools provided by the latter to respect human dignity and limit monitoring and surveillance.[54]

In artificial intelligence systems classified as high-risk, in which, drones result, the 'Human in the loop' principle, which provides for human oversight and supervision right from the design and development phase, is also guaranteed (see Art 14 AI Act).

If the principle of human oversight applies to drones, the same is not the case for the fundamental rights impact assessment under Art 27 of AI Act.

On this point, in fact, the AI Act provides for the possibility of carrying out an impact assessment of fundamental rights, but in a unilateral and compliance-oriented way, which does not seem to include drones, since Art 27 remains excluded from the regulatory perimeter of chapter III, sec II, AI Act, to which Art 108 AI Act refers. Art 2 para 2) AI Act provides, in fact, that to AI systems classified as high-risk, pursuant to Art 6, para 1, concerning “products” governed by the Union harmonisation legislation, listed in annex I, sec B, only, Art 6, para 1, articles 102 to 109, Art 57 and Art 112 apply.

In annex I, sec B, item 20 we find some areas of reference, among which Reg. (EU) 2018/1139 (Art 108 AI Act) is expressly mentioned, which refers to UAS, to be amended in Art 17, 19, 43, 47, 57, 58, in order to bring the products in line with the provisions of chapter III sec 2 of the AI Act, which requires certain conformity requirements for placing on the market or for their use.

---

[52] Regio Decreto 16 Marzo 1942 n. 262 on the approval of the Civil Code (Italy).
[53] European Agency for Safety and Health at work (n 6).
[54] The European Social Partners' Framework Agreement on Digitization available at <https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020_Agreement%20on%20Digitalisation%202020.pdf> accessed 5 November 2024.

These are a series of requirements to be fulfilled (Art 8), in particular, with regard to risk management (Art 9), data and data governance (Art 10), technical documentation (Art 11), transparency (Art 13), human oversight (Art 14) and IT security (Art 15).

Important remains, therefore, as a limit to the exercise of employer powers and for the purposes of assessing the risks inherent in the use of technology, the GDPR's protection system.

The reference is to the GDPR article 35 (DPIA), which remains one of the main instruments to be adopted before processing begins and which provides for the possibility of consulting data subjects and their representatives on the intended processing, in order to assess the impact of the processing in critical scenarios, such as those referred to in article 35, para 3.[55]

The DPIA under article 35 of the GDPR opens up an important dialectical opportunity with employees, not found in other disciplines.

In addition to Art 35, the GDPR has a special focus on the protection of rights contained in Art 32 on the security of processing in conjunction with Art 40 on voluntary codes of conduct, Art 25 on data protection by design and data protection by default, and certainly Art 88 GDPR.

The GDPR thus confirms itself as a regulation to ensure that even AI systems respect digital rights and workers' rights. It introduces specific rules to regulate the processing of workers' personal data in the context of work, with the burden of proof on the employer's side as to compliance and thus represents a bulwark of democracy, capable of controlling and limiting employer power, filling regulatory gaps, overcoming doctrinal and jurisprudential contrasts of national systems, such as the one concerning the interpretation and application of Art 4 of the Workers' Rights Statute, bringing back to unity and strengthening the system of protections.

In the dialectic between privacy protection and innovation, even Art 2 para 7) Artificial Intelligence Regulation expressly recognises the force attributed to the GDPR, which is considered superordinate to the former.

Art 2, para 7. of the Artificial Intelligence Regulation leaves Regulation (EU) No. 679/2016 unaffected, with the exception of Art 10 para 5 and Art 59 of the same Regulation, with the intention of introducing greater data protection measures through corrective measures and to avoid distortive effects and for the purpose of developing spaces for regulatory experimentation under Art 57, within which privacy and data are sacrificed for reasons of public interest.

[55] Art 35 paragraph 3 "A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9 (1), or of personal data relating to criminal convictions and offences referred to in Article 10; or © a systematic monitoring of a publicly accessible area on a large scale".

All of the above, together with respect for the principle of accountability, before adopting remote control tools, as well as respect for the general principles of processing (arts 5, 24 and 25 GDPR), so as to fully and exhaustively represent the processing before it begins means[56] contributing to the awareness of the data subject and to aspire to a result of reliable, person-friendly and socially accepted AI systems.

3 Drones and liability: limits of current regulation or lack of regulation?

The issue of liability is still unresolved and although the intention of the Community legislator is to develop a regulation with rules proportionate to the risk of each operation, the special rules of the Code of Navigation provide for strict liability which is mainly borne by the operator or the exerciser.

Article 874 of the Navigation Code, identifies the figure of the operator as the person who takes over the operation of the aircraft or the person responsible for events arising from the operation itself.

International regulations, on the other hand, identify the figure of the operator.

In the Riga Declaration of 06 March 2015 entitled "Framing the future aviation" it is reiterated that the "owner or operator" must always be identifiable.

Regardless of the definitions, the figures of the manager referred to in the international regulations or the operator of codified extraction, are both required to manage flight and systems activities. According to the prototypical Easa regulations, they are responsible for every aspect pertaining to the safety of the organisation, thus also for privacy, security, data collection, considered safety requirements for operations,[57] environmental protection, up to insurance obligations.[58]

This results in a very heavy liability on the part of the operator, albeit within the limits of the mandatory minimum insurance coverage.

[56] See GPDP, Provv. No. 364 of 06 June 2024, available at <www.garanteprivacy.it> accessed 10 June 2024; see also in Bolognini and Pelino (n 36) 490.

[57] See to that effect Reg. (EU) No. 1139/2018 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, Annex IX, Art 1, para 1 according to which Operators and remote pilots of unmanned aircraft are required to be familiar with national and Union rules on privacy, confidentiality protection, data protection, security, in order to ensure safe operations and separation distance between unmanned aircraft, persons on the ground and other airspace users. This provision is recalled by Recital 2 of the subsequent Delegated Regulation (EU) 945/2019 of 12 March 2019.

[58] Alpa (n 29) 921. According to the author, in the concept of indemnifiable unfair damage, interests particularly protected by law and corresponding to the most important values of society must be included: the values of the human person, on the one hand, and those of property on the other, identifiable with absolute subjective rights, which find direct recognition and protection in the Constitution. In this sense see also Amedeo Santosuosso, *Law, Science, New Technologies* (2nd edn, Wolters Kluwer 2016) 32 ff, who in citing Art 53 of the Nice Charter: Level of protection ie *"Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti … dalle Costituzioni degli stati membri; parafrasando il testo dell'articolo l'autore, dunque, afferma che in caso di contrasto tra Carta e costituzioni nazionali, non prevale la fonte astrattamente di grado superiore (e cioé la Carta), ma quella che garantisce il maggiore livello di protezione, di modo che la carta possa solo incrementare le tutele e mai limitare quelle esistenti a livello nazionale"*.

The position of the agent, if it coincides with the owner and/or responsibility of the processing, in the event of material or immaterial damage for breach of Regulation (EU) No. 679/2016 is, moreover, aggravated by further charges, pursuant to Art 82 GDPR, with the application of significant sanctions, which would seem to introduce liability for damages (material or immaterial) also by way of fault or intent (see Art 83, para 2 (b)), with reference both to the unlawful processing of data, but also and especially to the failure to adopt proactive behaviour.

In particular, the bridging rule, which allows liability profiles to be configured for the entire operation and therefore also for damage to persons and property, is that of Art 965 of the Navigation Code, and the rule generically speaks of aircraft in flight, referring to the typical scheme of strict liability.

Article 965 provides that the liability of the operator for damage caused by the aircraft to persons and property on the surface is regulated by the international rules in force in the republic, which also apply to damage caused on the national territory by aircraft registered in Italy. The same regulations also apply to State aircraft and equivalent aircraft referred to in articles 744 and 746.

We speak in a generic sense of aircraft and therefore also of UAS, and the assimilation of the latter to the category of aircraft allows the application of the code rules.

The compensation varies in relation to the weight of the aircraft (see Article 11 of the Rome Convention of 07 October 1952)[59] and thus there is a first limitation of the rule, which does not address the specific risk of the operation and clashes with other regulations, first of all with Regulation (EU) No. 1139/2018 and the subsequent implementing Regulations, but also with the AI Act itself, which intends to standardise the matter.

Even the new ENAC regulation of December 2021, which sought to align itself with European legislation, introduced three categories configured according to the hazard profiles of the operations (open, limited, certified) and the provision of specific compensation for the agent.

The weight criterion, the absence of specific risks for the purposes of commensuration of the indemnifiable damage, and the allocation of strict liability to the operator,[60] is not only inconsistent with other current legislation on the subject but is also out of time and not in line with technological development and also with the drone 2.0 strategy, which focuses on market and product development needs.

On the other hand, even in the rules of common law and specifically in the case of Art 2054 of the Civil Code (para 2), in the event of a maintenance defect or construction

[59] Convention on damage caused by foreign aircraft to third parties on the surface, signed in Rome 7 October 1952, hereafter Rome Convention.

[60] *Ceretti Vs. Crescini* [1997] Brescia Tribunal 28 July, according to which, in the event of the death of a passenger, the owner, who is not the driver of the aircraft, is not jointly and severally liable with the pilot, because aviation law does not provide for a principle such as that of article 2054 of the Civil Code, paragraph 3); the aircraft operator also lacks passive legitimacy, unless his capacity as a transport or charter company is proved.

defect, liability, although in the first instance falling entirely on the driver and jointly and severally on the owner of the vehicle, has been introduced as a residual rule, which some doctrine considers a *species* of the *genus* of corporate liability.[61]

In the case of drones, however, there may be problems introducing defective product liability to mitigate the effects of the special codicil rules, due not only to the absence of shared liability, similar to what happens in article 2054 of the Civil Code but also because the special codicil discipline prevails over all and on this point, it is necessary to reflect on the fact that the maritime sphere is the only one to have conferred a special position also on customs, which in the field under examination acquire a role equal and equal to that of ordinary laws.[62]

It follows from this that it is advisable to focus attention more on the codified rules already in force, hypothesizing an extension of them as regards the allocation of liability to various subjects in addition to the operator (who may be the owner, the person responsible for processing and not always the same as the employer), or rethinking a risk-based approach to liability, with the possible allocation of liability to various figures, such as the owner and the principal, developing specific situations on the discharge of the burden of proof as regards compliance with the techno-regulation, especially in relation to the phase prior to processing.

In summary, it is worth asking who takes the risk of dangerous operations, especially in the area of privacy and data security.

Only the operator or also the company that produced it, right down to the software designer and developer? It is also necessary to ask who is the operator in each operation and whether it coincides with the data controller and the employer.

All of the above confirms the importance of defining ex-ante the risks and making the most of what has already been established in Regulation (EU) 2018/1139 with regard to privacy and data security, which, among other things, provides for the principle of privacy by design, sharing it with the GDPR.

Another case of liability, subsumed under the heading of corporate liability, could occur in the case of the use of drones in production contexts, with infringement of the privacy and data security aspects of both the employees and the operator in charge of the mission. In such a case, the strengthening of the legislation should concern the allocation of liability to the operator, but also to the owner and the principal, identifying, on a case-by-case basis and in concrete terms, who is really the subject capable of affecting the processing of data.[63]

Transparency and the assessment and determination of risks in the case of drone operations could be based instead of adopting new rules by referring to new models, which can be tested from the sector in question, ie that of the working context.

[61] Alpa (n 29) 979 ff.
[62] Giovanna Visintini, *Nozioni giuridiche fondamentali: Diritto Privato* (Zanichelli Press 2021) 21.
[63] Ciucciovino (n 48) 955.

For the purposes of transparency and description of the context and devices used, it is also useful to resort to the voluntary codes of conduct under Art 40 of the GDPR, which would make it possible, due to their versatility, to avert the risk of technological development (which in the case of a defective product would entail penalizing consequences for injured parties due to the exemption of liability on the part of producers (see Art 118, letter e) of Legislative Decree No. 206/2005 of 06 September 2005)).

Such an instrument, especially if shared with the social partners from the outset or before treatment, would make it possible, to constantly adapt the product to the rules, map risks, including those in high-risk situations, circumvent the problem of special regulations on the one hand, while at the same time avoiding breaking the unity of the European regulatory system, especially in the area of techno-regulation, and could foster social acceptance of artificial intelligence systems, helping to mitigate strict liability, on a par with further accountability instruments.

3.1 From liability to accountability. The GDPR and the instructions supporting bargaining and consultation at the workplace

The combined provisions of articles 5 and 24 GDPR, fit right into the current European regulatory framework, which prefers an approach to the problems brought about by technological innovation, oriented towards risk rather than damage, in a dynamic of prevention rather than compensation and sanctioning. Precisely because of the speed with which the organisational and production changes linked to product manufacture occur, but also with regard to the contexts in which they are employed, the European legislator prefers to intervene at a physiological rather than pathological stage, in an attempt to avert burdensome budget items for companies and preferring to encourage, at the same time, the market needs to be linked to technological progress.

The criterion of the accountability of the data controller is understood as the one who has the capacity to determine in concrete terms the purposes and means of the processing referred to in Art 4, para 7, of the Regulation,[64] intersects with that of the employer, called upon in any case or even where it does not coincide with the owner of the processing to guarantee, on the basis of common law rules under Art 2087 of the Civil Code (which provides for a broader subjective scope than that of the GDPR), the psychophysical and moral integrity and therefore protecting the dignity of workers.[65]

The regulations referred to, one general and with a broader subjective scope providing for an obligation to protect, and the other more specific and pertaining merely to the ownership of the processing, share the principle of accountability, which is present at the organisational-managerial level, but also at the technical-operational level.

[64] ibid; see also personal data protection Authority, Provv. No. 9977020 of 11 January 2024, available at <https://www.garanteprivacy.it> accessed 10 March 2024.
[65] Alpa (n 29) 260.

The employer is called to answer if he has not taken all measures to protect the psychophysical integrity of the workers and is liable at least by way of *culpa in vigilando*, the burden of proof being solely on him. Similarly, the liability under Art 82 of the regulation, as well as that under the rules of the Navigation Code in the specific case of drones, provides for strict liability in the event that the rules of the regulation have been violated or proactive technical-organisational measures have been omitted, unless the owner proves that the damage is not attributable to him. Among the measures that help to perfect proof to the contrary, the Regulation provides for the demonstration of adherence to the codes of conduct under Art 40 or the certification mechanisms under Art 42 (Art 83, para 2 (j)). Account is also taken of the measures adopted to mitigate the damage (Art 83, para 2, (c)) and in particular of the technical and organisational measures referred to in Art 25 and Art 32 GDPR (Art 83, para 2 (d)), and this is for the purposes of the graduation of liability.

Adherence to the voluntary codes of conduct pursuant to Art 40 and recourse to the certifications pursuant to Art 42 GDPR, constitutes suitable elements for the fulfilment of the burden of proof, borne by the holder, of having complied with the obligations and measures, therefore also the proactive ones such as privacy by design, DPIA, Art 88, provided for in the GDPR.

3.2 Codes of conduct (referral)

The voluntary codes of conduct under Art 40 GDPR where adopted in production contexts, in order to have greater impact, should take into consideration, the opinion of the social partners, which is currently only envisaged as a possibility and is not mandatory (Cons. 99); by doing so they could really, constitute a hook with what is contained in Art 88 GDPR, but also in arts 25, 32 and 35.[66] Art 35 governs the data protection impact assessment and under para 8) the data controller is obliged to take codes of conduct into consideration when carrying out a DPIA, adherence to which helps to demonstrate, on the part of the controller, that appropriate solutions have been identified and implemented.

By means of the codes of conduct, the way for the adoption of proactive behaviour is reinforced and the procedure for the acquisition of informed consent by workers is also facilitated, restoring symmetry to the inequality inherent in it.

Consent is the legal basis for data processing especially where no other legal basis is provided, eg this happens in the cases already examined where the use of technology moves in a zone of uncertainty between paragraphs 1 and 2 of Art 3 of Legislative Decree No. 151/2015. In order to be free, informed, knowledgeable and above all unambiguous, it must give workers the opportunity to revoke it without prejudice, it must be subject to procedural simplification, possibly as when it was first given, traces of the consent must

[66] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational, safety and health. Recommendations to stakeholders' (2023), available at <https://osha.europa.eu> accessed 04 November 2023.

be kept, and it must be recorded and stored in order to trace back what and when workers consented. Consent can only be said to be free when there is real choice and, above all, control over monitoring.

For many of these aspects, codes of conduct, trade union agreements and impact assessment are appropriate instruments and strongly recommended also by the documents of the European Agency for Health and Safety at Work, in order to certify the correctness of the procedures adopted to protect privacy and for the social acceptance of complex technological systems.

The construction of a truly informed and conscious consensus on the product used in the work context, characterised by requirements of knowability, instead of unknowability, contributes to introducing elements of transparency and leads to a sharing of responsibility and widespread risk distribution for facts that affect the social sphere (such as health and safety). The latter are impossible to be taken care of solely and exclusively by the company, due to the high level of conflict they are capable of expressing and the high management costs associated with adapting to technological progress, as well as the multiplicity of regulations that accumulate different levels of liability.[67]

Transparency is an element that contributes to building a basis of trust with workers and is linked to the concept of fairness, equity and procedural fairness, as an element of rebalancing relations between the different subjectivities of the employment relationship (cf. Cons. 39 GDPR).

Managers and workers have the right to be informed about the collection and use of information concerning them and whether there are more or less hidden monitoring tools, the nature, purpose, and scope of which must be outlined. It is very important that workers, union representatives and managers know about the existence and functioning of AI and surveillance in the company.

Likewise, it is very important that there is adequate information on the use of such devices so that a clear representation of the processing carried out is provided to those concerned, before it begins and so that they are made aware of it.[68]

The high invasiveness of the processing necessarily corresponds to the timeliness of the information to the data subjects, who are asked to give their consent.

There is a thread that links procedural fairness to the knowledge and knowability of the product adopted, because only with timely knowledge is there a way to form an opinion

[67] Alpa (n 29) 950, according to which *"L'estensione della responsabilità d'impresa avanza con l'incremento della consapevolezza da parte dell'imprenditore dei suoi doveri sociali, con la composizione dei conflitti tra datori di lavoro e prestatori di lavoro, con l'acquisizione del consenso da parte dei consumatori, con la diffusione della coscienza ambientale. Aggiunge ancora l'autore Non credo sia possibile prevedere (…) una regola generale di presunzione di responsabilità; avrebbe maggior senso … la redazione di una regola generale di responsabilità per rischio, e quindi di responsabilità oggettiva. Ma si è visto che per ogni settore in cui si registrano danni derivanti dall'attività di impresa si riscontrano regole che presentano una loro peculiarità: regole che prevedono cause di esonero, ovvero prove specifiche, ovvero circoscrivono a taluni danni la responsabilità senza colpa, affidando poi al principio generale basato sulla colpa il regime ordinario di responsabilità"*.

[68] See GPDP, Provv. No. 364, of 06 June 2024, available at <www.garanteprivacy.it> accessed 10 June 2024.

in time and to give truly free and informed consent and, if necessary, exercise the right to object.[69]

Transparency, fairness, and timeliness are interlinked concepts.

Given the vulnerable position and the fragile nature of the consent expressed by workers, monitoring systems must be accompanied by a continuous discussion with the social partners and possibly shared with the workers, whose opinions should be constantly and carefully documented.

Through the codes of conduct, it is possible to identify the risks related to data processing, assess the origin, nature, likelihood, severity and the mitigation measures to be adopted, act as technical awareness-raising with regard to the regulation, determine the modalities and the concrete purpose of data collection, offer a cognitive framework of the technological products that will be used, facilitating, by anticipating it, the dissemination of knowledge of the product, so as to positively affect consent in terms of awareness, ensuring a concrete adversarial process with the interested parties.

Although not binding, moreover, once adopted they contribute to making market players trustworthy and less credible in the event of violation by customers, partners and employees, thus affecting the trust factor. Under Art 83, para 4 (c), moreover, an accredited supervisory body is subject to very heavy fines for "not having taken appropriate measures" in the event of a breach of a code of conduct by the controller or processor.

They are an additional tool to promote innovation, sustainable growth and risk minimisation, safeguarding data protection standards and customer confidence in the protection of personal data. They are an opportunity and not an end in order to concretely implement the principles of the GDPR, doing so in a shared way, to meet the needs of the market, of stakeholders, but also of employees (see also Cons. 78). Through the participation of the social partners, critical areas will in fact be highlighted and they will be able to know in advance and prepare for future bargaining topics. The contribution of technology is essential to restore value and dignity to the individual, doing so by means of the value (not necessarily the price) attributed to the data,[70] which are, finally, central to the bargaining processes between social and employer partners, not only in economic terms but also and above all in terms of improving living and working conditions as well as the overall enhancement of the discipline of Art 88 GDPR on bargaining, to be implemented in advance on the algorithm and subsequently on the data co-management.

[69] Gian Claudio Malgieri, *Vulnerability and data protection law* (Oxford University Press 2023) 38 ff, 132 ff .

[70] See also Vincenzo Ricciuto, 'Lo scambio dei dati con i contenuti e i servizi digitali: una nuova modalità di contrarre?' (2023) 1 EJPLT 20; Salvatore Orlando, 'Per un sindacato di liceità del consenso privacy' (2022) IV Diritto Persona e Mercato 527; Ilaria Amelia Caggiano, 'Il consenso al trattamento dei dati personali tra nuovo regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione' (2017) I Diritto Mercato Tecnologia 4; Francesco Gazzoni, *Manuale di diritto privato* (Edizioni Scientifiche Italiane Press 2003) 183.

4 Vulnerabilities in the GDPR and in the AI Act

The GDPR does not contain rules defining the worker as a vulnerable subject.[71] It is possible, however, to find traces of this in Cons. 43, which does not recognise consent as a valid legal prerequisite in the presence of a clear imbalance (of power) between the holder and the data subject, and in Cons. 42, which expressly mentions awareness as a requirement for the freedom of consent, placing the burden of proof on the holder to prove the formation of (valid) consent.

In the list annexed to the GPDP Order No. 467 of 11 October 2018, which in implementation of Art 35, para 4, indicates the types of processing to be subjected to the data protection impact assessment, referred to in Art 35, para 1 and Art 36, para 5, processing carried out in the context of the employment relationship, by means of technological systems, from which the possibility of remote monitoring of employees' activities is derived, is also mentioned, along with other non-occasional processing of data relating to vulnerable persons.[72]

In work contexts, there is an absence of balance and the doctrine traces the so-called vulnerabilities to relationships characterised by power asymmetry, where consent is originally flawed and not genuine.

This confirms what is already contained in WP 29, which traces vulnerability to a situation of imbalance of power or danger of high risk of harm, to fundamental rights and freedoms.

In order to bring such situations back into balance, first of all, a risk assessment of the excess of the processing is required, which can justify the limits to the freedom of the worker and the fundamental rights.

Secondly, it will be necessary to refer to other bases legitimising the processing (cf. arts 6 and 9 GDPR) or to reinforce the acquisition of consent with modalities capable of guaranteeing real and adequate information, which leaves workers free to form an opinion and possibly object to the processing, and therefore with the adoption of determined and predetermined procedures prior to the processing.

The AI Act, similarly to the GDPR, recognises without providing a definition, the vulnerabilities and takes into account the group vulnerabilities in Art 5. It therefore prohibits the placing on the market, commissioning, or use of AI that are intended to distort the behaviour of persons belonging to groups that are socially or economically disadvantaged and also prohibits the so-called social score. Art 5, para 1 (f) also prohibits the placing on the market, commissioning, and use of AI systems to infer a person's emotions in the workplace and educational establishments. In addition to prohibitions, the AI Act enhances product conformity through appropriate certification, accountability

[71] Malgieri (n 69) 87 ff, 115 ff.
[72] See in Bolognini and Pelino (n 36) 1382.

and compliance to respond to vulnerable situations. It makes accountability as objective as possible in order to protect the weakest.

The GDPR, on the other hand, responds to situations of vulnerability in two ways. The first aimed at implementing the principle of transparency (see arts 12, 13, 17), and the most important declination will be the information given to the interested parties; the second through a risk-based approach, similar to the AI act, ie with the provision of certain tools to create the conditions for transparency to be implemented.[73]

Some of these have already been examined in the course of this work and consist of the use of trade union agreements (Art 88), codes of conduct (Art 40) and DPIA (Art 35). Another very important tool is privacy by design under Art 25 GDPR, capable of guaranteeing the principle of minimisation (Art 5.1 (c) GDPR), linked to the principle of accountability and responsibility.[74]

Privacy by design not only constitutes a measure capable of exempting the data controller from liability profiles, but is also contained in the regulation on drones (EU) No. 1139/2018, which establishes the basic principles to guarantee security, privacy, and the protection of personal data, through the introduction of bureaucratic burdens, without losing sight of technological innovation in the civil aviation sector.

This regulatory framework gave rise to Regulations 945 and 947/2019, transposed by EASA and ENAC at the level of domestic law, which implemented the Aviation Strategy for Europe adopted by the Commission in 2015, which had as its objective the development of safe drone operations and legislation enabling the development of industry standards preordained for this purpose.[75]

5 Relevance of techno regulation and privacy by design for privacy and data security in regulation (EU) N. 1139/2018 and in art 25 GDPR. Juridical intersections with AI Act

The adoption of Regulation (EU) No. 1139/2018 was an important developmental moment in building a common European policy and framework on drones. It extended the scope of EU competence to all drones, without making distinctions on the basis of weight or size, as was the case in the previous regulatory framework, including the design, manufacture, maintenance, operation of propellers and engines, uninstalled parts, and equipment as well as equipment for remote control of unmanned aircraft. It contains a risk-oriented approach to all operations and by means of implementing and enforcing regulations and has sought to address the safety of operations through the use of

[73] Malgieri (n 69) 133 .
[74] On the principle of minimisation and privacy by design, see the decision of GPDP, Provv. No. 1712680 of 27 April 2010, which recommends the use of systems that are pre-set and allow anonymisation, available at <https://www.garanteprivacy.it> accessed 5 November 2024.
[75] An aviation strategy for Europe, COM. (2015) 598, available at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014DC0207&from=EN> accessed 5 November 2024.

technology regulation, of which privacy by design is one of the most important declinations.

According to Regulation (EU) No. 1139/2018 fundamental requirement for drones is to "have the relevant specific features and functionalities that take into account the principles of privacy and data protection by design and by default" in order to "mitigate the inherent security risks to the protection of privacy to the protection of personal data, security, environment arising from their operation". So, there is an express reference to privacy by design, just as there is in Regulation (EU) No. 679/2016 (GDPR). The latter, however, cuts across all areas of technology use and therefore refers to processing whether it takes place on or off the platform. It is a regulation that aims to give citizens, in general, back control over their personal data, in a system, such as the current one, of digital and collaborative economy.

Article 2 of the GDPR is called the "material scope" and represents a novelty in the regulatory landscape because rather than distinguishing between subjective and objective scope, it takes care to specify in para. 1) that it "applies to the wholly or partially automated processing of personal data and to the non-automated processing of personal data contained in a file or intended to be contained therein".

Adhering to techno-regulation also means following the rules of privacy by design ex Art 25 and 42 GDPR, which will ensure that the dictates of the law are incorporated into the software of the robotic agent, so as to prevent unwanted acts[76] and to do so throughout the entire life cycle of the product.[77]

In the area of interest, drones, which can be likened to robots, can follow the European Commission's Robolaw Guidelines.[78] According to the dictates contained therein, certain principles such as informed consent, encryption and data access control can be integrated already at the design stage. The principle of minimisation (Art 5 GDPR) and purpose of processing may also be contained therein and continuously updated.[79]

With Commission Delegated Regulation 945 of 12 March 2019 on Unmanned Aircraft Systems and Third Country Operators of Unmanned Aircraft Systems, it is reiterated in Cons 1 and 2 that it is diriment for UAS, belonging to the open category of operations, to define, in advance, the risks arising from the operation of the devices, by referring to a framework of common and harmonised EU rules instead of referring to "classical" aeronautical compliance procedures. Cons 2 specifies that the said requirements should correspond to those in Art 55 of the Unmanned UAV Regulation No. 1139/2018, which should, in particular, take into account the specific characteristics and functionalities

[76] Merla (n 20) 44.
[77] Aude Cefaliello, Phoebe V Moore and Robert Donoghue, 'Making algorithmic management safe and healthy for workers: addressing psychosocial risks in new legal provisions' (2023) 14(2) European Labour Law Journal 117.
[78] European Commission's Robolaw Guidelines available at <https://www.robolaw.eu> accessed 10 December 2023.
[79] Merla (n 20) 35 ff. It is worth quoting the author's thought that *"il trattamento illecito dei dati personali ben può dipendere dal modo in cui il drone è stato disegnato o costruito, dalla negligenza del fornitore di connettività o di coloro i quali sviluppano determinati applicativi"*.

necessary to mitigate the risks inherent to flight safety, privacy protection, personal data protection or the environment arising from the operation of UAS.

Article 1 of the Delegated Regulation of March 2019 No. 945 provides that the Regulation is intended to establish requirements for the design and manufacture and of the additional remote identification components. For the requirements, it makes a reference to parts 1-6 of the annex, which is absorbent of the UAS remote control software devices, which according to part 6, would be those of direct remote identification.

The techno-regulation in Regulation No. 945/2019 also applies to the design, manufacture, maintenance and operation of unmanned aircraft to be understood to extend to software as well as engines and propellers. The use of terms such as "remote identification systems", would leave no room for doubt, a circumstance also confirmed by technical advice from engineers in the field.

This could also give rise to further liability profiles in the event of product malfunctioning, in addition to that of the operator, and thus configure (in the future) defective product liability hypotheses, also with reference to the violation of privacy regulations.

Assessing in advance and in a shared manner risk profiles and dangers inherent in automated activities, as required also in article 11 "Rules for the assessment of operational risks" of the subsequent Implementing Regulation (EU) No. 947/2019, concerning rules and procedures for the operation of unmanned aircraft, contributes to better delineate liability profiles and mitigate the strongly objective connotation, based on the special rules of the sector of the Navigation Code.

The regulations set out in Regulations (EU) No. 679/2016 and No. 1139/2018 also share the concept of privacy by design. The latter measure, in particular, in Art 55 refers for requirements to annex IX, for the mitigation of risks arising from security, privacy, data protection, environment, to be protected through specific purposes and characteristics by design and by default.

The Artificial Intelligence Regulation (see Art 108) amends, by supplementing it, Regulation (EU) No. 2018/1139, with the standards set out in chapter III sec. 2 of the AI Act. These rules concern high-risk systems and provide for corresponding compliance standards, which, in addition to providing for risk assessment and mitigation measures, must be designed in such a way as to ensure human oversight during their use (see Art 14).

The latter standard, although not aimed at workers, nevertheless intends to protect fundamental human rights and lays the foundation for ethically oriented robotics, which also seems to cover drones.

Considering that Art 69 of the AI Act also takes into account privacy by design and the value component of design by requiring the protection of personal data during the entire product life cycle and in a way that respects the principle of minimisation by design and by default.

In line with the considerations already made on the Artificial Intelligence Act and the vagueness of the rules on strict liability, which need to be adapted to the needs of the market and technological development, inherent in the drone sector (see also Strategy 2.0) Regulation (EU) No. 1139/2018 and the following 945 regulating the use of drones in the different flight scenarios as well as 947 on design requirements production and sale, as supplemented by the AI Act, are confirmed as essential tools to ensure the respect of fundamental rights, by means of adherence to the rules set forth in the GDPR and to continue to promote technological innovation and the market, promoted by the AI Act, which has as its legal basis arts 16 and 114 Treaty on the Functioning of the European Union.[80]

The application to drones of only the rules concerning the areas of regulatory experimentation (see Art 57 AI Act) confirms this assumption and opens up the possibility of experimental regimes, without prejudice to the application of liability rules.

5.1 Drones and sandbox. Article 57 of the AI Act

The techno-regulation, standardisation, and the product-oriented approach find a favourable scenario in the development of sandboxes, which are useful to address security problems and can remedy the rigidity of conformation, which could be a blocking factor for the development of the market and the sector.

The Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, in Art 2 para 1, classifies drones in high-risk AI systems and consequently considers only certain provisions applicable to them, the most important of which is article 57, which governs sandboxes, limited to cases in which the requirements for high-risk AI systems, pursuant to the regulation, have been incorporated in such union harmonisation legislation.

Article 3, para 55, defines "regulatory AI test space" as "a controlled framework established by a competent authority that offers providers or potential providers of AI systems the opportunity to develop, train, validate and test, where appropriate in real-life conditions, an innovative AI system, in accordance with a test space plan, for a limited period of time under regulatory supervision".

Article 3, para 54, on the other hand, defines the trial space plan, functional to the former, as a document agreed between the participating supplier and the competent authority in which the objectives, conditions, timetable, methodology and requirements for the activities carried out within the trial space are described.

They can be regarded as persuasive measures on a par with Codes of Conduct and co-regulation, whereby certification procedures are created for an early assessment of the risk brought by the technology being trialed.

[80] European Commission, 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe' COM(2022) 652 final, available at <https://www.ec.europa.eu> accessed 10 October 2024.

Unpublished rules are sought that are studied and tested for individual cases and considered concretely rather than abstractly, in order to arrive at new technological solutions, in which market efficiency passes through legal certainty because participation in the sandbox does not exempt participants from liability, for damage caused to third parties as a result of experimentation within it.

Pursuant to para 12, suppliers and participants of the experimentation spaces in the experimentation phase remain in any case and in fact liable under Union and national law for damages caused to third parties as a result of the experimentation taking place in the experimentation space.

Critical points of sandboxes are the indiscriminate use of personal data (see Art 54, para 1 AI Act), which, however, should not apply to drones, given the narrow scope of application of the regulation in Art 57 AI Act, and the legal and market fragmentation, with impact on product standards.[81]

The strengthening of the strict liability profiles from which the sector already suffers and which would confirm the technicality of the AI Act, oriented to product conformity rather than to better delineate liability profiles more functional to the market, are another of the critical points that characterise this legal institution.

5.2 Allocation of liability between regulatory developments and recommendations. New organisational models or new rules?

In 2019, the Commission adopted two implementing regulations.

Regulation (EU) No. 945/2019, in particular, establishes the technical requirements for unmanned aircraft, namely: product requirements for design and manufacture; obligations of economic operators importers and distributors; presumption of conformity requirement as well as type of drone whose design, manufacture and maintenance will be subject to certification; implementation of drones intended for use in the "open" category and remote identification add-ons; drone operators from third countries when conducting drone operations pursuant to the implementation Regulation (EU) No. 947/2019 within the single European sky space.

Regulation (EU) No. 947/2019, on the other hand, sets out detailed conditions for drone operations, including requirements for (remote) pilot qualification and airworthiness, risk assessment, cross-border operations, registration of the drone and its operator, competent authority.

[81] See Statement by Austria expressed at the Council's approval of the AI Act on 15 May 2024, which expresses concern about the indiscriminate use of personal data in the sandboxes provided for by the regulation, as the wording is considered vague and general and not suitable as a solid legal basis for the processing of personal data under Article 6 (1) (c) GDPR and would not comply with the principle of minimisation, as it lacks limits as to the scope of the processing and categories of personal data potentially processed available at <https://data.consilium.europa.eu> accessed 23 June 2024.

National competent authorities are required to establish and maintain registration systems for drones (whose design is subject to certification) and drone operators (whose operation may pose a risk to safety, security, privacy, and the environment).

Once again, the centrality of the operator is confirmed also for privacy and personal data protection aspects, who, under the special codified regulations, is the only responsible party.

The ENAC Reg. of 04 January 2021 referred, generically, to the GDPR for the respect of privacy (see Art 29).

The vagueness and residual nature of these regulations is mainly due to the absence of a penalty system in the event of violations, a circumstance that once again confirms the centrality and relevance of GDPR.

For privacy aspects, in particular, operators, where they operate in a specific and certified category, will be required to register and display their registration number on the UAS. The same rule is applicable in the case of open category where the weight of the UAS exceeds 25 KG or in any case if equipped with a sensor capable of detecting personal data.

Registration is an administrative procedure to which Art 14 of Regulation (EU) No. 947/2019 and 6 ENAC, link the qualification of drone operator (operator according to the aeronautical approach).

The principle of privacy by design and by security, which we find regulated both in Reg. (EU) No. 679/2016 and in Reg. (EU) No. 1139/2018, is a burden on designers and economic operators, pursuant to Reg. (EU) No. 945/2019 and which the National Authorities are obliged to verify before proceeding with the conformity certifications referred to in Reg. No. 947/2019.[82]

Both Regulations are required to comply with the provisions of Chapter III sec. 2 of the Artificial Intelligence Regulation, which provides for uniformity burdens on providers of high-risk AI systems, including drones.

The GDPR proves to be the most significant regulation in the current EU legislative landscape. In addition to prohibitions, it deals mainly with processing and provides rights for data subjects as well as duties for specific categories of persons, such as data controllers, who in the workplace do not always coincide with the person responsible for the drone operation.

With respect to processing, there are in fact in advance forms of protection based on proactive and widespread conduct and next, by means of remedies of a private,

[82] See to that effect Regulation (EU) No 679/2016 of the European Parliament and of the Council of 27 April 2016 concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46/EC [2016] OJ L119/1, Art 25 and Reg. (EU) No. 1139/2018 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency [2018] OJ L212/1, Art 55 and Annex IX, Art 1.3, according to which the basic requirement for drones is "*Possedere le relative caratteristiche e funzionalità specifiche che tengano conto dei principi della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita*".

repayment and compensatory nature,[83] with which the system intends to remedy unlawful processing under articles 82 and 83. The latter article inserts a fault-based liability, also based on the failure to adopt measures, such as privacy by design, the presence of which in some cases excludes liability (see Art 82, para 2) in others limits liability (see Art 83, para 2 (d and j)).

5.3 Codes of conduct and bargaining as functional tolls for consensus building, implementation of transparency and risk mitigation

The 2015 Riga Declaration on Drones had raised the issue of insurance, liability and compensation schemes for victims, affirming the need to develop norms inherent to technologies and standards capable of ensuring the integration of drones in the airspace. The voluntary codes of conduct under Art 40 of Regulation (EU) No. 679/2016, could help in the elaboration and configuration, concretely and in advance, of risk situations. The compulsory consultation of social partners and stakeholders, currently provided for only on an optional basis, could be the condition to make this tool truly effective for privacy protection purposes and beyond.[84]

Not only would transparency be enhanced, but also the acquisition of consent [85] would be truly informed, free, responsible and aware,[86] becoming a true and proper act of manifestation of will, from which to start evaluating the lawfulness of processing,[87] instead of being limited to a merely authorizing scheme.[88]

The codes of conduct under article 40 GDPR, are confirmed as useful, versatile and authoritative self-regulatory instruments due to their legitimacy at the public level (i.e., the approval of Public Supervisory Authorities, under Art 55 Reg. (EU) No. 679/2016 and Cons. 122). They allow for the introduction of compulsory consultation of the social partners and lend themselves to regulate any situation involving the use of technologies, including high-risk technologies, such as may be those related to data processing in production contexts. Once developed and approved, they can be used by suppliers to demonstrate compliance with the obligations brought by the GDPR, including for the

[83] Lucilla Gatt, Roberto Montanari and Ilaria Amelia Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Politica del diritto 351.

[84] See to that effect Regulation (EU) No. 679/2016 of the European Parliament and of the Council of 27 April 2016 concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46/EC [2016] OJ L119/1, Considering Art 99, which employs the verb "*Dovrebbero*" in relation to consultation by data controllers, of data subjects, when drafting, amending and extending Codes of Conduct.

[85] Federica Paolucci, "Consenso, intelligenza artificiale e privacy. Commento a: Corte di Cassazione, sez. I Civ. – 25/05/2021, n. 14381" (2021) 1 MediaLaws <https://www.medialaws.eu/consenso-intelligenza-artificiale-e-privacy-commento-a-corte-di-cassazione-sez-i-civ-25-05-2021-n-14381/> accessed 25 October 2024.

[86] A Davola, 'L'acquisizione di dati da parte dei privati nelle operazioni con SAPR' in Erica Palmerini, Maria Angela Biasotti and Giuseppe Francesco Aiello (eds), *Diritto dei droni. Regole, questioni e prassi* (Milano 2018) 149.

[87] Orlando (n 70) 527.

[88] *Movimento Federativo Democratico Vs. Associazione Bancaria Italiana Banca Popolare Coop.a ARL Banca Fideuram Spa* [2000] Rome Tribunal available in Corriere Giuridico 00 496, mentioned in Gazzoni n 70 183.

purposes of discharging the burden of proof in the event of damages for breach of privacy and data breaches.[89]

Where there are data protection impact assessments to be carried out pursuant to Art 35 GDPR, as in the case of the use of artificial intelligence and particularly innovative and pervasive technologies, such as drones, with enormous potential, in future scenarios, in terms of surveillance, predictive analysis, profiling[90] and assessment of the individual, up to more sophisticated forms of monitoring inherent in automated processing, the adoption of the code of conduct (Art 35, para 8), will help to make the product more knowable and understandable and thus may have a positive impact on transparency.[91]

The codes of conduct in Art. 40 GDPR, unlike those in the AI Act (see Art 95), do not provide for the limitation of adoptability in low-risk situations and are therefore of wider application, ie in situations characterised by the use of technology, in general.

Also the Recommendation CM/Rec (2015) 5 of 1 April 2015, of the Committee of Ministers to Member States on the processing of personal data in the employment context, urges to bear in mind principles such as data protection and respect for private life and to "promote the acceptance and application of the principles set out in the appendix of the soft law document, through supplementary instruments such as codes of conduct so as to ensure that these principles are known, understood and applied by all persons in the employment sphere, including employers' and employees' representative bodies, and that they are taken into account in the design and use of ICT in the employment sphere".

The agreements with the social partners under Art 88 of the GDPR confirm this last meaning and are therefore suitable for defining the framework and the protection of fundamental rights, to safeguard the individual, through the negotiation carried out *ex ante* and *ex post*, i.e. in terms of bargaining on the constitutional values that regulate the algorithm and in terms of data co-management (determination of the purpose of processing, access, portability, transfer, modification and revocation of consent, right to rectification and control of data accuracy). The latter, above all, will be of great importance in very specific situations such as, for instance, the filming of workers for company promotional and advertising purposes.

Bargaining understood in this way will be able to have a significant impact on the quality of life of workers, impacting on working time and working hours in the company for example (so-called work life balance), and on the improvement of working conditions in a broader sense.[92]

[89] European Commission, 'New Rules for Artificial Intelligence - Questions and Answers' (2024), available at <https://commission.europa.eu> accessed 02 January 2024.
[90] Guido Noto La Diega, 'Machine rules. Of Drones, Robots and the info-Capitalist Society' (2016) 2 The Italian law Journal 401.
[91] *Filcams Cgil Torino Filt Cgil Torino Ndil Cgil Torino Vs. F.S.R.L.* [2023] Turin Tribunal 05 August, 6.
[92] Alessia Maccaferri, 'Sostenibilità, al centro la qualità della vita e del lavoro' *Il Sole 24 Ore* (25 February 2024) 20. According to the author, sustainability is increasingly understood as quality of life and work, and 89% of companies are increasingly interested in social sustainability, first and foremost internally, by committing themselves to improving the quality of life and work of their employees.

This, among other things, will be instrumental in overcoming the typically contractual scheme, based on the exchange and price of data, understood as goods to be regulated.[93]

Consent thus understood will not be ascribable to an act of private autonomy, but not even to a mere acknowledgement, but will be a truly free authorisation, because it will be conscious and informed, aimed at obtaining control over data and benefits not strictly related to economic value, the use of which will be the employer's responsibility in terms of accountability. This will allow for a balancing of interests, such as that (but not only) of profit-sharing for those concerned, allocating precise liabilities to the parties, mainly employers.[94]

The European Social Partners' Framework Agreement on Digitisation, while affirming the validity of technology in the company to guarantee and protect the health and safety of the working environment and workers, at the same time, reaffirms that the dignity of the human being, which could be violated when subjected to surveillance or performance monitoring systems, must be safeguarded, expressly mentioning collective agreements as the appropriate instruments to implement Art 88 GDPR, so as to enable workers' representatives to address data, consent, privacy and surveillance issues.

To this end, it will be important to link the collection of data to a concrete and transparent purpose that is, above all, current and not generically determinable in the future.

6 Conclusions

There is a unifying legislation on drones at EU level, contained in the aforementioned regulations, extensively commented on in the previous section.

The international discipline assimilates and conforms under the regime of special provisions, aircraft and drones in an all-encompassing manner; the intersections with other regulations have been examined, and at the same time, thanks to the contribution of Regulation (EU) No. 1139/2018, the need to rethink a risk-based approach has been raised, in order to configure liability cases also with regard to privacy and data security.

The current legislation has a number of limitations, including an excessive concentration of liability entirely on the operator, especially in the case of drones used for civil purposes, the extent of the damage commensurate with the weight and not with the concrete risks related to the operation, and therefore not in line with current market development needs; lastly, the legislation is generic in terms of privacy and acquisition of consent, and lacks a sanctioning apparatus, with respect to which reference should be made to the GDPR and the AI Act, limited to suppliers for high-risk artificial intelligence

[93] Salvatore Orlando, 'Il Coordinamento tra la Direttiva 2019/770 e il GDPR. L'interessato consumatore' (2023) II Persona e Mercato 232.
[94] Alessio Gramolati, *Contrattare l'innovazione digitale, Una cassetta degli attrezzi 4.0* (Ediesse S.r.l. Press 2019).

systems. In production contexts, where drones are mostly work tools, problems arise with regard to the allocation of liability on different subjects and not only on the operator and therefore also on the principal, who does not always coincide with the data controller and the owner

The employer is called upon, however, to answer, pursuant to Art 2087 of the Civil Code to the workers and is therefore obliged even before the start of processing to follow the principles of accountability and compliance, of privacy by design, resorting to advance consultation and negotiation, so as to do everything possible to guarantee the rights of the persons concerned.

The concept of privacy by design is a widespread aspect in all the disciplines examined and constitutes one of the most evolved aspects of the design of AI systems, beyond techno regulation. It is supposed to be shared with software developers and manufacturers, but also with suppliers, as is the case in high-risk AI systems.

It takes place before processing. Therefore, it must be promoted by data controllers and processors, but already at an earlier stage, and therefore necessarily also involves software developers and designers, making use of the GDPR's support tools, such as impact assessment, to incorporate certain constitutional and treaty values, such as those of privacy, data protection, non-discrimination, and transparency, within and from the outset.[95]

This reading is confirmed by Art 2 of GDPR called “material scope”, which seems to introduce a diffuse type of liability, ascribable to a very broad scope within which the concept of 'processing' also falls.

For this purpose, the importance of the techno-regulation present in all the disciplines referred to, from the GDPR to the regulations standardizing the matter up to the AI Act, which confirm the importance of the accountability dimension in a system centred on a strict liability. This absolute dimension of liability also reaffirmed in Art 57 of the AI Act on the spaces for regulatory experimentation, which strongly inhibits the market and is not able to respond incisively, like the GDPR, to situations of vulnerability, such as those concerning the protection of workers' data and privacy.

It is the company's burden, moreover, to demonstrate that it has taken all the measures set out in the GDPR when processing workers' data by means of the technology used in the company, and it will therefore be in the company's interest to demonstrate that it has adopted the proactive behaviours set out therein and the risk mitigation measures. The latter are to be found in Cons. 71 (processing accompanied by appropriate safeguards such as information, right to human intervention, prohibition of automated processing, expressing one's opinion and guaranteeing an adversarial process, right to an explanation, right to challenge, appropriate mathematical or statistical procedures for profiling, technical and organisational measures for correcting data inaccuracies, minimizing the

[95] Orlando (n 70) 538.

risk of errors, avoiding discriminatory decisions), in Cons. 78 for privacy by design, in Cons. 77 for codes of conduct, which, together with the agreements with the social partners under Art 88, contribute to the acquisition of consent, by means of procedural models appropriate to the risk.

Art 88 of the GDPR while respecting the guarantee rules of the domestic legal system and collective agreements such as Art 4 of the Statute of Workers' Rights, intends, with a forward-looking and forward-looking approach, to regulate the purpose of the collection and the use that will be made of the data, through unprecedented technological systems, seeking to avoid discrimination and violations of privacy and the identity of the worker from the outset.[96]

We can then understand why it is necessary to guarantee the knowledge and knowability of the algorithm, as well as the importance of recognising and incorporating constitutional values immediately from the design stage, that is, from the moment when the algorithms are put into the system and the data that qualitatively meet certain characteristics are chosen, in order to make the predictive and surveillance systems work, both on the platform (by means of automated processing and profiling) and off, as in the case of drones and artificial intelligence surveillance systems in general.

One therefore grasps the importance not only of the codes of conduct ex Art. 40 GDPR and the DPIA, but also of the collective bargains ex Art 88 GDPR, both in terms of algorithm bargaining and in terms of data co-management, and thus the importance of bargaining both in advance and next and during the entire product life cycle.

With the advancement of technological equipment and telematic resources that broaden the possibility of control over the worker, which can also take place by computer, national regulations must be adapted. Article 88, para 1, responds to this need and delegates to collective bargains the possibility of introducing bargaining aimed precisely at work organisation, management and planning. Para 2 further specifies that such agreements will be adopted to ensure transparency of processing, protection of dignity, where there are data transfers and in the case of the adoption of workplace monitoring systems.

The contribution of technology will have a significant impact on the bargaining of the future, increasingly focused, in the writer's humble opinion, on time and space at work, with relevant benefits for workers' freedom, quality of work and work-life balance, beyond and despite the pervasiveness of surveillance.

The adoption of new regulatory models will serve to re-establish fairness and restore symmetry to relations, together with the identification of higher legitimate interests, such as those of health protection, which alone can justify the use of invasive technologies and data processing, but which can become an easy pretext for improper and instrumental use against objectively weaker and more vulnerable subjects, such as workers.

[96] Santosuosso (n 58) 346 ff.

One understands, therefore, the reason why the Artificial Intelligence Regulation has re-proposed privacy by design and compliance, including drones among the high-risk systems, and has provided for the standardisation of regulations for them to bring them into line with the main rules concerning them, first and foremost the principle of human oversight.