

Personal data and discriminatory risks in smart mobility systems

Utilizzo dei dati personali e rischi discriminatori nei sistemi di smart mobility

[DANIELA MARCELLO](#) 
Senior Researcher
University of Florence

Abstract

Smart mobility systems promote efficient, safe, and sustainable transportation of goods and people through the use of AI and the Internet of Things, such as smart cars, smart roads, intelligent traffic controllers, and much more. They require constant and extensive data collection for their operation. This paper analyses the Italian-European regulatory landscape and relevant guidelines, and examines the risks of violation of privacy and discrimination associated with the algorithmic processing of such extensive information as that collected by smart mobility systems.

I c.d. sistemi di smart mobility promuovono sistemi di trasporto di beni e persone che siano efficienti, sicuri e sostenibili mediante l'uso dell'IA e dell'Internet of Things, come per esempio le smart cars, le smart road, i regolatori del traffico c.d. intelligenti e molto altro. La caratteristica consiste nel fatto che essi esigono per il loro funzionamento una costante e imponente raccolta di dati. Il lavoro analizza il panorama normativo italo europeo e le linee di indirizzo sul tema e svolge una riflessione sui rischi di lesione alla riservatezza della persona e rischi discriminatori connessi all'elaborazione algoritmica di informazioni così imponenti come quelle trattate dai sistemi di smart mobility.

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.

This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
<https://creativecommons.org/licenses/by-nc-nd/4.0/>



Keywords: personal data; big data; algorithms; IA; smart mobility; discriminatory risks; smart car;

Summary: [1. Smart mobility systems and processing of personal data.](#) – [2. The Italian-European regulatory scenario.](#) – [3. Big data, algorithms and personal data.](#) – [4. Discrimination risks.](#)

1. Smart mobility systems and processing of personal data.

Emergencies related to climate change, biodiversity loss, environmental degradation, and pollution clearly demonstrate how the intensive or harmful exploitation of natural resources directly harms human life, health, and economic well-being, while also threatening the survival of future generations. This growing awareness has led to the promotion of policies that support the planned and optimized use of both human and natural resources, including through artificial intelligence technologies and systems¹. In recent years, sustainable urban development has become a central focus of European policies, with technology playing a crucial role in this regard. Terms such as “smart city”, “smart building”, and “smart governance” are used to identify synergies between technology, regulation, and infrastructure, to enhance system efficiency, environmental protection, and overall quality of life². In Italy, cities such as Milan, Bologna and Rome are lead in digital innovation with significant growth in the Internet of Things (IoT) and sensor technology; in recent years, in this cities it is registered a 30% increase in the deployment of sensors and a 40% rise in control centers for mobility, urban security and energy consumption monitoring platforms in public buildings³.

Within this framework, smart mobility systems aim to ensure efficient, safe, and sustainable transportation of goods and people through the use of AI and the Internet of Things. These systems include smart cars, smart roads,

¹ The term ‘sustainability’ was first used and defined in an official United Nations document in 1987, in the Brundtland Report (named after its coordinator, Gro Harlem Brundtland, and entitled ‘Our Common Future’), published by the World Commission on Environment and Development (WCED), which states: ‘Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs.’

In 2015, ‘sustainable development’ became the priority of the United Nations Sustainable Development Goals for the year 2030. As European Commission President Ursula von der Leyen noted in her speech on 9 May 2021 at the launch of the Conference on the Future of Europe, the contributions of European citizens are essential to addressing key issues such as health, good and sustainable jobs, and climate change in an increasingly digital economy, in order to shape the Europe in which they wish to live. All 27 EU Member States have committed to making the EU the first climate-neutral continent by 2050; to this end, they have pledged to reduce emissions by at least 55% by 2030, compared to 1990 levels. The new Social Climate Fund will support EU citizens most affected by, or at risk of, energy poverty or mobility poverty. Furthermore, see Regulation (EU).

² N. Casiddu, “RAISE e(co)-cities. Ecosistemi, nuove tecnologie e sviluppo socioeconomico in reti multi-urbane”, *Techne*, (Florence, 2025), 30118–127; E. Giorgini, “Città, edifici intelligenti e benessere” (2024) 2, *Tecnologie e diritto*, 373; Aa.Vv., “Smart cities. Diritti, libertà e governance” by Matteo Giannelli e Valentina Pagnanelli, (Torino, 2023), 18 e ss..

³ EY Report Smart City Index 2025, aprile 2025, in https://www.ey.com/it_it; Osservatorio sulle tendenze e le applicazioni del supercalcolo, *La mobilità del futuro Tendenze e applicazioni del Supercalcolo, Big Data e Quantum Computing* by Eleonora Ocello - Eleonora Barelli, (Aprile 2024), 25. R. P. Dameri, A. Cocchia, “Smart City and Digital City: Twenty Years of Terminology Evolution”, *Proceedings itAIS 2013 - X Conference of the Italian Chapter of AIS*, 2013, 1, <http://www.itais.org/proceedings/itais2013/pdf/119.pdf>.

advanced traffic management tools, and much more. A defining characteristic of such system is their reliance on continuous and extensive data collection. They collect, match and use: location data, as the GPS tracking, they are used to provide navigation services, but also to track the movements of motorists and, with the advent of artificial intelligence, to move cars in the space; driving behavior data such as acceleration, braking, cornering and others which are used to improve vehicle safety and efficiency, but also to track drivers' driving routine and automatically control traffic flows; environmental data such as temperature, humidity and other data are used to improve passenger comfort, but also to track weather conditions or activate rain or fog mechanism, and so on; passengers' data, such as their ID, movements and conversations⁴.

The operation of smart cars and smart cities requires interactions that generally include vehicle-to-vehicle (V2V) communication, vehicle-to-infrastructure (V2I) or infrastructure-to-infrastructure (I2I) communication, and communication between vehicles and pedestrians or cyclists (vehicle-to-everything, V2X). The term C-ITS (Cooperative Intelligent transport Systems). There is an acronym, usually used, that is C-ITS (Cooperative Intelligent Transport Systems), which can be defined as a peer-to-peer solution for the exchange of data between vehicles and other transport infrastructure (road signs or other transmission/reception stations) without the intervention of a network operator⁵.

Beyond operational data, these systems also process additional information to improve performance and provide services commonly referred to as infotainment for example, some mobile phone applications may allow users to locate parked vehicles or monitor vehicle condition remotely for preventing breakdowns. And it is easy to imagine that the enhanced development of AI systems will lead to an even greater increase in the amount of data used. In fact, investing in on-board telematics makes it possible to offer new services. For example, there are prototypes of self-driving Yamaha motorcycles without handlebars, which, thanks to an integrated AI system, recognize their owner, reach them, and follow their movements. Obviously, it can do this thanks to the use of data, specifically thanks to a biometric identification system, through which it recognizes the owner and receives commands via their body movements even if the driver is not on the motorbike.

⁴ S. Battiston, *L'evoluzione della smart city in smart community: Strumenti di collaborazione tra P.A. e soggetti privati per il perseguimento degli obiettivi del P.N.R.R.* (Italia, Key Editore, 2023), 13; M. C. Gaeta, "Green and Sustainable Mobility in Road Transport: How Private Law Can Guarantee the right balance between Environmentally Sustainable Development and digital transformation", (2023), 34, n. 1 *European Business Law Review*, 63-80; T. Favaro, "Verso la "smart city": sviluppo economico e rigenerazione urbana", (2020), 2, *Riv. giur. edil*, 87; A. Simoncini, "IA e smart cities", in M. Giannelli e V. Pagnanelli *Smart cities, Diritti, libertà e governance*, (Torino, 2023), 3.

⁵ On 30 November 2016, the European Commission adopted a European Strategy on Cooperative Intelligent Transport Systems (C-ITS) (Brussels, 30.11.2016 COM(2016) 766 final, available at <https://eur-lex.europa.eu/>), a key initiative towards cooperative, connected and automated mobility. The strategy was the result of work carried out through the platform for the deployment of C-ITS systems in the European Union (C-ITS platform, established in November 2014 as a Commission expert group), an operational tool for dialogue, the exchange of technical knowledge and cooperation between the Commission, public stakeholders in the Member States, local/regional authorities and private stakeholders such as vehicle manufacturers, equipment manufacturers, road operators, telecommunications operators and service providers. The aim of the C-ITS Strategy is to facilitate the convergence of investments and regulatory frameworks across the EU, in order to enable the deployment of C-ITS services.

The defining feature of smart systems is their connectivity, which enables continuous data exchange. In fact, in the guide 'Cyber security and resilience of smart cars'⁶, the European Union Agency for Network and Information Security (ENISA) defines smart cars as vehicles equipped with systems that provide connected features designed to enhance the user experience or improve vehicle safety through the use of telematics, connected infotainment or in-vehicle communication. The report emphasizes that the prerogative of such systems is in their connected functionality and therefore in their ability to collect, join, and transmit data; this entails risks linked precisely to the ability of smart cars to share information. Among these risks, the Report highlights those relating to the danger of surveillance and violation of user privacy; it suggests, as good practices useful for containing threats, calling on suppliers to identify all data processed relating to an identified or identifiable person; this call is addressed not only to manufacturers but also to subcontractors or suppliers, all of whom are required not to process user data more than necessary; it also identifies as a general rule that service providers other than the manufacturer should be prevented from accessing user data that has not been anonymized or pseudonymized, unless such data transmission has been obtained with the user's consent; finally, it calls for enhanced authentication measures to enable controlled and controllable access by the user⁷.

AI systems and smart cars, therefore, require a continuous exchange of information, which, if implemented with statistical inference systems, leads to highly risky results, since data that may seem insignificant, when connected to other data, can offer unexpected predictive results.

2. The Italian-European regulatory scenario.

The analysis begins with an examination of certain important measures, including the so-called Ecall Regulation issued on 29 April 2015⁸ and EU Regulation 2019/2144 (RUESicProt)⁹, Italian law about so called Smart Road¹⁰ and Guide Lines 01/2020¹¹ about the processing of personal data in the context of connected vehicles, which contribute significantly, together with other so-called soft law measures from supervisory authorities or working groups within

⁶ ENISA, "Cyber security and resilience of smart cars", 13 gennaio 2027, in <https://www.enisa.europa.eu/>

⁷ "Resolution on data protection in automated and connected vehicles", https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf; "Connected Vehicles", <https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/>.

⁸ Regulation (Eu) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, in <https://eur-lex.europa.eu>

⁹ Regulation (Eu) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users,, in <https://eur-lex.europa.eu>.

¹⁰ D. M. 28 February 2018 (Italian Decree so called Smart Road), in Gazzetta Ufficiale 18 April 2018 n. 90.

¹¹ Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications Version 1.0 Adopted on 28 January 2020 by European Data Protection Board (EDPB), in <https://www.edpb.europa.eu/>

institutional bodies, to define the regulatory framework of the issue considered¹².

Well, starting with the so-called Ecall Regulation issued on 29 April 2015 by the European Parliament, it has been mandatory since spring 2018 for all newly manufactured vehicles to be equipped with an automatic system capable of automatically calling for help in the event of particularly serious accidents.

The eCall system is defined in Article 3 of the Regulation as 'an emergency system, consisting of in-vehicle equipment and means to activate, manage and implement the transmission of an eCall, triggered automatically by in-vehicle sensors or manually, which sends, via wireless mobile communication networks, a minimum set of data and opens a 112-based audio channel between the vehicle occupants and a PSAP for the eCall service'. The legislator, fully aware that data protection requires the regulation and supervision of both data collection and storage, has included a specific article on data security (Article 6), and takes care to specify that the unique purpose for which the data is processed is to deal with emergencies, so the data must be stored only for the period of time necessary to deal with the aforementioned emergencies and to be completely deleted as soon as it is no longer necessary for that purpose. Furthermore, according to the principles of privacy by design and by default established by the GDPR¹³, manufacturers are required to comply with a telematic security standard, as the 112-based on-board ECall system must not be traceable or subject to constant monitoring, and data must be automatically and continuously deleted from the system's internal memory. May be stored only the last three positions of the vehicle, strictly to indicate the current position and direction of travel at the time of the event. Ultimately, the use of technologies that ensure greater privacy protection is required in order to provide ECall users with an adequate level of privacy protection, as well as the necessary safeguards to prevent surveillance and abuse.

As regards EU Regulation 2019/2144 (RUESicProt), its objective is to significantly reduce the number of deaths and serious injuries on the roads by requiring vehicles to be equipped with certain technologies relating to the safety and protection of vehicle occupants and other road users, which also operate through the use of data.¹⁴ The Regulation imposes a basic set of safety technologies for cars, e.g. intelligent speed adaptation, alcohol interlock devices¹⁵ or event data recorders (EDRs). Obviously, even in this case, it is clear

¹² E. Bertelli, "La giustizia predittiva nella Twin Transition", (2024), 2, *Tecnologie e diritto*, 286.

¹³ Art. 25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

¹⁴ Cfr. Goel R, Tiwari G, Varghese M, Bhalla K, Agrawal G, Saini G, Jha A, John D, Saran A, White H, Mohan D. Effectiveness of road safety interventions: An evidence and gap map. *Campbell Syst Rev.* 2024 Jan 3;20(1):e1367. doi: 10.1002/cl2.1367. PMID: 38188231; PMCID: PMC10765170. The study analyses research, interventions and legislative measures adopted in high-income countries to improve road safety. Indeed, road traffic injuries (RTIs) are among the top ten causes of death worldwide, accounting for 1.35 million deaths each year, of which approximately 93% occur in low- and middle-income countries. Despite numerous global resolutions to reduce road traffic accidents, their numbers have continued to rise in many countries. The study aims to assess the external effectiveness of the approach adopted by countries that have successfully pursued road safety policies, with a view to promoting its adoption in low- and middle-income countries that are currently developing their road infrastructure.

¹⁵ Law No. 177/2024, which amended the Highway Code (Articles 125 and 186) and introduced a requirement for all drivers convicted of drink-driving to install an alcohol interlock device (blood alcohol

that the data produced can also be useful for tracking driver habits and, through this, again for the statistical and predictive functioning of artificial intelligence, even any unintended results. It is enough to consider, quite simply, that alcohol interlock systems record data such as the blood alcohol level detected in every breath test – both at start-up and whilst driving – as well as the exact time and date of every ignition attempt, whether the test was passed or failed, and any resets whilst the vehicle is in motion. Some devices take a photo at the moment of the breath test to confirm the driver's identity and prevent someone else from taking the test in the driver's place; others, more advanced, track the vehicle's location at the time of tests or lockouts. This data could enable user profiling, or aggregated data could reveal the habits of groups within a specific geographical area or belonging to a particular ethnic group.

In Italy, Law No. 205 of 27 December 2017 (2018 Budget Law) is also important, as it provides for support, including financial support, for the dissemination of good technological practices in the digital transformation process of the national road network, the so-called (SMART ROAD) project. For the law implementation the Ministerial Decree, approved on 28 February 2018, provides for two steps: the first by 2025 for work on the infrastructure of the entire road and motorway network; the second by 2030 for the activation of services such as traffic diversion, intervention on average speeds to avoid congestion, structural monitoring of the stability of motorway works, and more. This decree was updated in 2020 to include autonomous vehicles. The project has been led by ANAS, which has already installed sensors on the main roads under its jurisdiction to enable communication between cars and smart roads. There are several locations equipped with smart cameras that enable the geolocation of vehicles; when all services are fully operational, there will be a continuous and massive exchange of information, the cameras will constantly monitor traffic, and it will also be possible to locate vehicles carrying dangerous goods to ensure they are travelling in accordance with regulations.¹⁶

Finally, the Guidelines 01/2020 on the processing of personal data in the context of connected vehicles and its applications, adopted on 9 March 2021, are an important document that provides a detailed overview of the state of the art up to 2020, highlighting how the processing of personal data in the context of connected vehicles can serve a variety of purposes, including driver safety, the provision of insurance services, the optimization of transport systems, as well as entertainment and information services. These Guidelines are in accordance with the principles of the GDPR; consequently, they require that the data processing need to ensure that the purposes of any data processing are specified, explicit, and legitimate, and that any subsequent

level between 0.8 and 1.5 g/l (mandatory use for 2 years) and those caught with a level exceeding 1.5 g/l (mandatory for at least 3 years, subject to possible extension by the Local Medical Commission). The requirement applies to all vehicles used by the person penalised, and the costs of installing and operating the device are borne entirely by the driver (Ministerial Decree of 2 July 2025, published in the Official Gazette No. 171 of 25 July 2025, set out the technical specifications and installation procedures)

¹⁶ To monitor the implementation of the smart roads initiative, the Smart Roads Observatory was established at MIT in 2018. Regarding the status of projects launched (completed and ongoing) under the decree D.M Smart Road cfr L. Maci, *Smart road, che cosa sono le strade intelligenti del futuro e a che punto siamo in Italia*, 2025, Nextwork360 - Boosting Tech Company Growth, in <https://www.economyup.it/>

processing of the data is not incompatible with the original purposes, and that there is an adequate legal basis (Article 5 of the GDPR). Furthermore, they reinforce the principle of data minimization by requiring vehicle manufacturers, service providers and other data controllers to limit the collection of personal data to only that which is relevant and necessary for the purposes pursued; particular protection is required for location data, as it can easily reveal the lifestyle habits of data subjects and therefore, their collection should take place only when strictly necessary to avoid a high degree of intrusion into the user's private life. The importance of providing users with clear information, implementing secure authentication mechanisms, and taking all other necessary measures to ensure data protection is also emphasized, because the connected vehicles generate a very high volume and variety of data. Consequently, the technologies used should be designed to minimize the collection of personal data, adopt privacy-by-design settings, and ensure that data subjects are adequately informed, as well as being able to easily adjust the settings relating to the processing of their data¹⁷.

It is clear from the above that the rules of GDPR are applied to all data relating to natural persons, especially rules about the accountability regime for data controllers, and about privacy by design and privacy by default; whereas the GDPR doesn't apply to the anonymized data, which falls within the scope of non-personal data¹⁸. In the event of termination of the contract, the trader must refrain from using any content other than personal data (which remain subject to the provisions of the GDPR) that has been provided or created by the consumer in the course of using the digital content or digital service provided by the economic operator, unless such content has been aggregated by the economic operator with other data and cannot be disaggregated, or at least not without disproportionate effort.

This approach certainly has a clear framework, but it presupposes that it is easy to distinguish between personal and non-personal data – a distinction which, in reality, is by no means straightforward when it comes to the algorithmic processing of such vast amounts of information as that collected or capable of being collected by smart mobility systems. In this context, it is necessary advocating for a shift in perspective: from focusing solely on personal data to considering data more broadly as a central element of the digital economy. This approach emphasizes the need to regulate not only data collection and processing but also the outcomes of algorithmic systems, including their potential to influence behavior and decision-making.

¹⁷ In 2014, the European Court of Justice also strongly emphasized the principle of proportionality as a fundamental criterion for balancing security requirements and the protection of individuals. It criticized the Data Retention Directive 2006/24/EC, adopted following the attacks in London and Madrid in 2004 and 2005, which harmonized European legislation on the retention of telephone conversations and electronic communications traffic to ensure their availability for investigative purposes, and ruled that the general and indiscriminate retention of data was unlawful. (Court of Justice, 8 April 2014, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, at <https://eur-lex.europa.eu/>).

¹⁸ Regulation (Eu) 2023/2854 of the European Parliament and of The Council of 13 December 2023 on harmonised rules on fair access to and use of data, Art. 3: « Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user.»

3. Big data, algorithms and personal data.

It is clear that the challenge remains unresolved: the risk of mass surveillance, user profiling and the use of data which, although not immediately traceable to a specific individual (whether identified or identifiable), nevertheless reveal that person's routine and lifestyle does not appear to be easily addressed simply by attempting to separate personal data from non-personal data¹⁹. The AGCOM²⁰ has effectively highlighted that the quality of data (whether personal or non-personal) also depends on the underlying purpose of data processing, as well as on any search for correlations and the increasingly widespread use of algorithms and machine learning techniques, going so far as to say that: 'the characteristics of data also depend on "the eye of the beholder"'. Therefore, our thinking cannot remain tied to the traditional concept of data, as a disposable or non-disposable asset, solely because it relates to an identified or identifiable person²¹.

In fact, the legal experts who first examined privacy issues relating to the use of smart cars immediately highlighted that the distinctive feature of this phenomenon lay in the significant capacity of so-called smart cars not only to store operational data associated with the vehicle's use to improve performance, but also to exchange the information gathered in real time with the network, with personal devices, with other cars or with intelligent systems integrated into the infrastructure²². Every interaction with a smart device is transformed into information, which can then be used in various ways: to develop predictive models, to improve the device's performance, and to identify consumers' attitudes, tastes, and preferences. All of this generates an immense volume of data characterized by its heterogeneity, as it originates from diverse sources such as computers, mobile phones, the internet, sensors and mobile devices, etc.; by volume; by speed, thanks to the exponential increase in connections and the use of networked devices; by ubiquity, given the potentially unlimited expansion of data within the global network; and, finally, by possible inaccuracy, due to a lack of verification of the authenticity, accuracy and quality of the information. It can thus be observed that algorithmic reasoning, AI systems, and predictive models are capable not only

¹⁹S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, (Roma, 2019), 22. The author describes surveillance capitalism as something unique and distinct from any form that preceded it: a new contest where space and time follow their own logic and, as a result, cannot be understood using existing concepts; Z. Bauman, D. Lyon, *Liquid surveillance*, (Cambridge, 2013), 9; M. Saeudy, AM. Gerged, K. Albitar, "Accounting perspectives on the business value of big data during and beyond the COVID-19 pandemic", (2022), vol. 21 n. 2, *Accounting & Management Information Systems / Contabilitate si Informatica de Gestiune*, 174-199; P. Chung-Lien, L. Ya, P. Yu-Chun, "Research on the Status of E-Commerce Development Based on Big Data and Internet Technology", (2022), vol. 13 n. 2, *International Journal of Electronic Commerce Studies*, 27-48; Y.N. Harari, *21 lezioni per il XXI secolo*, (Firenze, 2019) 419; A. Adinolfi, A. Simoncini, *Protezione dei dati personali e nuove tecnologie*, (Napoli, 2022), 130; M. Ferrari, *Alea e rischio nella realtà digitale*, (Napoli, 2022) 44.

²⁰AGCOM, *Big data Interim Report* Resolution no. 217/17/CONS, in www.agcom.it

²¹About the threats to personal privacy arising from the circulation of non-personal data E. Capobianco, G. Perlingieri, M. D'Ambrosio, *Circolazione e teoria dei beni*, (Napoli, 2021), 290.

²²A.C. Nazzaro, "Privacy e smart mobility", in Diana Cerini, Andrea Pisano Tedesco, *Smart mobility, smart cars e intelligenza artificiale: responsabilità e prospettive* (Torino, 2019) 50; M.G. Losano, "Verso l'auto a guida autonoma in Italia", (1 aprile 2019) II, 2, *Diritto dell'informazione dell'informatica*, 423.

of collecting, setting, and grouping information, but even of generating it through matching data and the circulation of so-called metadata, that is, through all that usage-related information that remains on the consumer's devices or the history of web browsing activities²³.

These operating systems, which underpin the information-based business models used by technology entrepreneurs, call for better and more effective protection of individuals²⁴. As some legal scholars point out²⁵, whilst until now the regulation of personal data processing has held a dominant position both in terms of the hierarchy of sources and scientific discourse, today a multipolar vision is emerging in which the centrality of personal data is being replaced by the centrality of data understood as any digital representation of acts, facts, and information. In this context, if the defining feature is the communication and exchange of data, then it does not seem possible to resolve the issue by addressing only the question of lawfulness/unlawfulness under the GDPR, and this for some reasons. Among these reasons is undoubtedly the widespread use of personal data, which is reshaping the issue of controlled data circulation, because consent does not always guarantee the data subject control over their data, and the legal basis for processing often proves elusive, particularly due to the vagueness of the purposes of the various processing operations to which the data are subjected²⁶. As we have seen, in smart mobility systems, the protection of users' personal data does not relate solely to the connection between vehicles and personal devices, but also to the data exchanged with

²³P. Perlingieri, "Diritto civile e intelligenza artificiale", (2025) 1, *Tecnologie e diritto*, 135. In order to prevent the misuse of artificial intelligence, the author calls for greater transparency, understood as the ability to identify the methods used for data collection, the processes on which they are based, and the reasons that justify them; G. Cerrina Feroni, *Intelligenza artificiale e ruolo della protezione dei dati personali*, intervento a Key4biz 14.02.2023; D. Iacovelli, M. Fontana, "Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici", (2022) III, *Il diritto dell'economia*, 107-138; G. Contaldi, "Intelligenza artificiale e dati personali", (2021) V, *Ordine internazionale e diritti umani*, 1193-1213; M. Tresca, *Lo «stato digitale» big data, open data e algoritmi: i dati al servizio della pubblica amministrazione*, (June 2021) fasc.2, 1, *Rivista Trimestrale Diritto Pubblico*, 545.

²⁴Legal scholars have long highlighted the paradigm shift that new technologies – and AI in particular – have brought about in the protection of privacy. In 1995, Stefano Rodotà warned that the debate on privacy did not merely reflect the traditional concern for the defense of the private sphere, but marked a significant qualitative shift that compels scholars to consider privacy within the broader context of the organisation of power, S. Rodotà, *Tecnologie e diritti*, (Bologna, 2021) 2nd stamp 33,97. Data collection today stems primarily from all the digital traces left in the digital environment through the use of information technologies and/or detected through the interaction between technologies designed for the digital processing and transmission of various types of information. Thus, social media, internet service providers, search engines, personal devices and anything capable of tracking online activity act as data collectors; furthermore, through the use of profiling techniques and complex algorithms, it is possible to extract additional information from users, which may relate to both personal and non-personal data. About big data R. Messinetti, "La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata", [2019] *Contr. Impr.*, 861; A.C. Nazzaro, "L'utilizzo dei Big data e i problemi di tutela della persona", (2018) 4, *Rass. dir.civ.*, 1239; L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il modo*, (Milano, 2017) 106; D. Cardon, *Che cosa sognano gli algoritmi, Le nostre vite al tempo dei big data*, (Milano, 2016) 70; C. Talamo, N. Atta, C. Martani, G. Paganin, "The integration of physical and digital urban infrastructures: the role of "Big data"", (Jun. 2016) 11, *TECHNE - Journal of Technology for Architecture and Environment*, 217–225; L. Edwards, "Privacy, security and data protection in smart cities: a critical EU law perspective", (2016) 2, *European Data Protection Law Review*, 28.

²⁵G. Resta, "La regolazione digitale nell'Unione Europea - pubblico, privato, collettivo nel sistema europeo di governo dei dati" (1 december 2022), fasc.4, *Rivista Trim. Diritto Pubblico*, 971.

²⁶N. Miniscalco, *L'intelligenza artificiale in movimento: l'impatto sui diritti costituzionali della smart mobility*, (Milano, 2024), 120.

other cars and with IT systems integrated into road infrastructure – and this is done not only for commercial purposes, but also for safety reasons. These mechanisms lead to an expansion of the scope of computability and drive an incredible acceleration in the process of society's digitalization, fueled by vast databases of information that have never before been so easily expandable and accessible. The development of algorithms that instruct computers to sort, process, aggregate, and represent information is such that it enables sophisticated predictive techniques, influences behavior, and encourages automated decision-making processes. The problem thus becomes broader and more profound, extending even to the fundamental principle of equality; indeed, automated decision-making processes and digital scoring mechanisms, even when designed to ensure equal treatment, can have serious discriminatory effects.

4. Discrimination risks.

In 2023, the European Union Agency for Fundamental Rights published a report warning of the risks of discrimination and the threats to fundamental rights posed by the use of artificial intelligence mechanisms, which undoubtedly include those described above. It refers to the Digital Services Act, which contains various provisions aimed at strengthening the protection of fundamental rights, and requires very large online platforms to assess risks to fundamental rights and introduce mitigation measures regularly. It suggests that better access to data held or generated by online platforms should be guaranteed to enable supervisory bodies and independent, qualified researchers to assess risks to fundamental rights.

The IA Regulation ²⁷ prohibits the placing on the market, putting into service or use of AI systems for the assessment of individuals or groups of individuals based on social behavior or known, inferred or predicted personal or personality characteristics, where the social score thus obtained results in: discriminatory or unfavorable treatment of specific individuals or groups of individuals in social contexts that are not linked to the contexts in which the data were originally generated or collected; discriminatory or unfavorable treatment of specific individuals or groups of individuals that is unjustified or disproportionate to their social behavior or the severity thereof. Such systems, or others that assign a social score to natural persons through algorithmic reasoning, may lead to discriminatory results and may also infringe the right to dignity, in which case they are prohibited. This prohibition, however, does not affect lawful practices of assessing natural persons carried out for a specific purpose in accordance with European Union law and the national law of individual Member States. In the transport sector, one critical issue that has already emerged concerns the use of AI and big data to determine motor insurance premiums. The personalization of policies means that risk assessment is based on customer-specific information such as the frequency of

²⁷ Regulation (Eu) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, in <https://eur-lex.europa.eu>

vehicle use, driving style, and the routes taken (which may involve roads with high or low accident rates)²⁸.

The factors that may be used to provide a comprehensive and accurate assessment of risk, for example, the insured person's driving and lifestyle habits, should not relate to aspects of private life and, above all, should not create categories of higher risk based on ethnic, gender, or geographical grounds²⁹. However, the risk of discrimination does not only concern the identification of disadvantaged or minority groups or categories, but also the formulation of pricing policies that exclude certain individuals from the insurance market because they are considered high-risk, thereby undermining the principles of mutual assistance and solidarity on which the insurance market is founded³⁰. The greatest risk associated with algorithmic reasoning is consistency taken to extremes, through logical reasoning based on the technique of repeating results assimilated from the past, which may perpetuate discrimination, and the technique of syllogism, which leads to erroneous arguments or arguments flawed by a statistical objectivity that takes reasoning out of context and disregards ethical values³¹. Another risk is the quality of the data collected, which, as already mentioned, may be incomplete, inaccurate, outdated, or untruthful. For example, some studies have found that car safety systems (seatbelts, headrests, and airbags) are designed primarily based on data from crash tests using dummies modelled on the weight and body dimensions of men; consequently, women's breasts, their body shape, or pregnancy are not taken into account. This has significant consequences in terms of the severity of injuries sustained in accidents, as it appears that women are 47% more likely than men to suffer injuries in road accidents and are consequently penalized in terms of policy costs; it also appears that they are 17% more likely than men to die in a similar accident³².

It is therefore clear that the current phase of development in data protection law is bringing about a profound reshaping of the global economic order, in that, for the first time, people's everyday experiences – across all areas of social life – are being systematically harnessed as essential inputs for economic

²⁸ IVASS, *Indagine sull'utilizzo degli algoritmi di Machine Learning da parte delle imprese assicurative nei rapporti con gli assicurati*, March 2023, in www.ivass.it. The survey involved 93 insurance companies (all Italian companies and four non-EU companies) and was conducted between June and September 2022 to explore the use of Artificial Intelligence (AI), ML and other technologies, and the use of ML algorithms to build risk clusters in which to classify vehicles and geographical areas, in order to determine the tariff coefficients used in calculating premiums.

²⁹ S. Landini, "Data sharing and innovation in the insurance industry" (2025) I, *European Journal Privacy Law & Technologies*, 1-12; A. Fabris, "Algorithmic Audit of Italian Car Insurance: Evidence of Unfairness in Access and Pricing." Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society. New York, NY, USA: ACM, 2021. 458-468. Web, 460; E. Giorgini, "Profilazione automatizzata e contratto assicurativo", (2024) 4, *Assicurazioni - Rivista di diritto, economia e finanza delle assicurazioni private*, 751; A.C. Nazzaro, "Macchine intelligenti (smartcars): assicurazione e tutela" [2018] *Dir. merc. ass. fin.*, 77.

³⁰ A.C. Nazzaro, *Big data and segmentation of price*, <https://hdl.handle.net/20.500.14090/1128>.

³¹ About gender gap J. Gerards, R. Xenidis, *Special Report «Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law»* by European network of legal experts in gender equality and non-discrimination, Lussemburgo, 2021.

³² C. Schabasser, "AI discrimination trap? - Recommendations for combating discrimination against women through AI." (2025) 9, *London Journal of Social Sciences*, 11-19. <https://doi.org/10.31039/ljss.2025.9.31>; C. Niethammer, "AI Bias Could Put Women's Lives at Risk - A Challenge for regulators", (27 May 2020) <https://www.forbes.com/sites/carmenniethammer/2020/03/02/ai-bias-could-put-womens-lives-at-risk-a-challenge-for-regulators/>.

models based on practices – which are often opaque – of mass data collection, extraction and processing³³.

Such practices serve the purposes of commercial profiling and the marketing of goods and services, but also the design and direction of processes for developing prevention and security systems, as well as the assessment of conduct and the construction of reputational systems, such as so-called digital scoring, with the consequent difficulty of distinguishing between algorithmic systems that create reputational profiles and personalize the offer of goods or services, and those which, on the other hand, by exceeding the aforementioned limits, discriminate against and prejudice certain categories of individuals. For this reason, the point raised by careful legal scholarship appears fundamental³⁴: we must also consider the output of algorithmic reasoning, namely that 'quid novi' generated by the aggregated use of diverse and extensive types of data, as well as whether or not it is intended for circulation. In doing so, the protection of the individual is not limited to algorithmic reasoning that involves personal data, but also extends to algorithmic calculations based on non-personal data, which are nevertheless put into circulation for a specific purpose and which involve aspects of the protection of the individual or their self-determination.

Perhaps the oversight and control mechanisms should operate on several levels: firstly, and perhaps most importantly, the level relating to the risk profile, for which it would be important to make the information, simulations and studies on which the ex ante assessment of data processing risk is based accessible to the supervisory authorities in the relevant sector, to verify and monitor the 'privacy by design' mechanisms adopted; the second, relating to the storage and possible disclosure of data to prevent it from being used for other purposes; processing policies should make it transparent and easily discernible which third parties the data is disclosed to; the third, relating to information for users, who should be clearly and effectively informed of the operations and processing carried out on the information in connection with the privacy-by-design mechanisms adopted thirdly, regarding information for users, who should be clearly and effectively informed about the operations and processing carried out on information relating to their personal activities, even when the data processed is not personal; finally, it would be desirable for all activities involving an assessment of the user's conduct (from the evaluation of driving style to the riskiness of the user's habits and so on) to always be supervised by a human assessor who can contextualize and evaluate the specific case to prevent discriminatory assessments. The above is consistent with the regulatory framework governing data processing and the protection of individuals within the axiological context of our legal system; however, the challenge lies in effectively implementing the principles of equality and the protection of individuals, rather than reducing them to bureaucratic tasks which, on the one hand, hinder the flow of data (now a valuable asset in the

³³ A. Simoncini, *Intelligenza artificiale e futuro delle libertà costituzionali*, in *Intelligenza artificiale e futuro delle libertà costituzionali*, (Soveria Mannelli, 2021).

³⁴ C. Perlingieri, *Creazione e circolazione del bene prodotto dal trattamento algoritmico dei dati*, in *Il trattamento algoritmico dei dati tra etica, diritto ed economia* (Atti del 14° Convegno Nazionale 9-10-11 maggio 2019 Grand Hotel Vesuvio Napoli) (Napoli, 2020), 177 ss.

digital economy) and, on the other, prevent users from gaining awareness, which, on the contrary, appears necessary for the data subject's collaborative participation in the use and protection of their own data.

To effectively address these challenges, a multi-level approach to oversight is necessary. This includes enhanced transparency in risk assessments, stricter controls over data storage and sharing, clear and accessible information for users, and the incorporation of human oversight in automated decision-making processes. Ultimately, the goal is to ensure that technological innovation aligns with fundamental principles such as human dignity, equality, and individual autonomy, without reducing data protection to a purely formal or bureaucratic exercise.