**ITALY**



***MINISTRY OF FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION***

***inter-ministerial committee for human rights***

**ITALY’S CONTRIBUTION**

**ON RIGHT TO PRIVACY IN THE DIGITAL AGE**

*May 28, 2021*

**ITALY’S CONTRIBUTION**

[privacy-report@ohchr.org](mailto:privacy-report@ohchr.org)

registry@ohchr.org

Italian Authorities are in a position to provide the following contribution, **for your information only**.

**(Source: Italian Data Protection Authority - *Garante per la protezione dei dati personali***)

The Italian Data protection Authority (Garante per la protezione dei dati personali) is honoured to provide its contribution for the preparation of the thematic report on artificial intelligence, including profiling, automated decision-making and machine-learning technologies which may, without proper safeguards, affect the enjoyment of the right to privacy. Without claiming to be exhaustive and remaining available for any further needs and information, it would like to share the following remarks with regard to the three submitted questions:

**1)The specific impacts on the enjoyment of the right to privacy caused by the use of artificial intelligence, including profiling, automated decision-making and machine-learning technologies (hereinafter referred to in short as “AI”) by governments, business enterprises, international organizations and others.**

***Preliminary remarks (2,273 words)***

*Machine-decisions are mostly based on the collection and processing of personal (and non-personal data) which render the application of data protection principles inevitable and central for the setting up of adequate safeguards for the rights of the individuals. The right to private life and to the protection of personal data as enshrined by international and regional legal instruments is indeed the expression of the individual’s self-determination and autonomy which must be preserved in a scenario where the decision-making is more and more allocated on machines.*

*Existing data protection instruments already provide an essential basis for the regulatory exercise on artificial intelligence. For example, both EU and Council of Europe data instruments, respectively the GDPR and Law Enforcement Directive, and the Convention 108+ provide for some specific rules which are particularly relevant in the AI scenario such as:*

*- the right of the individual not to be subject to automated decisions (Article 22 of the GDPR, Article 11 of the LED and Article 9.1.a of Convention 108+);*

*- transparency obligation and the right to know the logic of the processing, particularly relevant in a context where the decision-making mechanisms can be opaque and unintelligible for the data subjects impacted by the automated decision making (Article 15 GDPR, Article 9 Convention 108+);*

*- Data Protection Impact Assessment – DPIA (Article 35-36 GDPR; Article 27 LED; Article10 of Convention 108+);*

*As for the said data protection instruments, even not explicitly mentioned, many provisions are relevant to AI, and some are indeed challenged by the new ways of processing personal data that are enabled by AI. There is indeed a tension between the traditional data protection principles (purpose limitation, data minimisation, the special processing of 'sensitive data', the limitation on automated decisions) and the full deployment of the power of AI and big data”.*

**a) relevant technological developments, the driving economic, political and social factors promoting the use of AI and the main actors in and beneficiaries of deploying and operating AI (developers, marketers, users);**

*We highlight that the involvement of all stakeholders of the AI systems (developers, marketers, users) and the assignment of roles and responsibilities is of great value to ensure a full protection of individuals’ rights impacted by AI. In the allocation of roles and liabilities, the consistency of such roles with the ones of data controller and data processor set forth by data protection legal tools should be duly considered to facilitate a coherent application of different legal frameworks.*

*Regarding the definition of the main actors of AI value chain it is relevant that, in compliance with a participatory model, civil society, and in particular of those groups potentially affected by AI applications, is duly involved in the choices regarding the adoption of AI solutions to facilitate the detection and removal of existing bias and discrimination.*

**b) ways, in which AI can help promote and protect the right to privacy;**

*Generally speaking, the protection of the right to privacy (as well as of several other fundamental human rights) can be fostered to the extent a human-centric AI is aimed at. This entails that AI systems and technologies are developed from the start in a way that is consistent with fundamental human rights; as regards the rights to privacy and data protection, this entails that a data protection by design and by default approach is used when developing AI systems that are intended for or rely on the processing of personal data for specific purposes, and that the ex-ante assessment of AI-related risks includes data protection implications;*

*More specifically, one could envisage AI-based applications that can help controllers and processors in performing, in particular, the required Data Protection Impact Assessment (DPIA); this would be especially helpful in complex situations requiring multiple input (risk) factors to be considered. DPIA can benefit from risk analysis tools based on AI provided that the outcomes are not enterely left to the machine and on the contrary is subject to human intervention. [….]*

*AI systems can be valuable tools to enhance the security of data, which is one important component of the protection of personal data. AI can indeed be used to detect security breaches, leaks or other accidents, provided that the data protection requirements are respected. […].*

**c) challenges posed by the use of AI for the effective exercise of the right to privacy and other human rights, including features and capabilities of AI that present existing or emerging problems;**

*There are persisting challenges posed by the use of AI for the effective exercise of the right to privacy:*

*the peculiar features of AI, substantially different from the human approach which is mostly based on causal reasoning, renders transparency a particularly difficult goal to achieve as it may not necessarily lead to a prior intelligible explanation of the results made by the machine. It is of the utmost importance that new tools, more proactive and timely, are developed in order to ensure that pre-warnings on potential harm is given thereby allowing the individual to react and eventually modify the decision. It is moreover crucial to develop new instruments capable to avoid a bureaucratic vision of information and privacy policy to be provided to individuals. This, having in mind that transparency is key as regards AI and impacts also the possibility / feasibility of meaningful consent (where applicable) to the processing of one’s personal data via AI technology (right to explanation, but not only that).*

*With regard to the need to ensure human intervention in the decision making allocated on machines, appropriate mechanisms must be provided to ensure the effectiveness and qualification of human intervention. What is indeed essential is that the human called upon to break the machines’ determinism is qualified, competent and free enough to allow an efficient departure from what would have been automatically decided by the machine.*

*What is also needed is to foresee a human right precautionary principle meaning that before the deployment of AI systems a careful assessment is carried out on the impact of those systems on human rights, including the right to private life and the protection of personal data.*

*Finally, the use of AI for public interest purposes (including surveillance in specific contexts) requires specific legislation and such legislation should detail safeguards to enable exercise of data protection/privacy rights (e.g. deferral of exercise for limited period, provision of alternatives/fall-back options, etc.)*

**d) discriminatory impacts of the use of AI;**

*AI enables automated decision-making even in domains that require complex choices, based on multiple factors and non-predefined criteria. In many cases, automated predictions and decisions are not only cheaper, but also more precise and impartial than human ones, as AI systems can avoid the typical fallacies of human psychology and can be subject to rigorous controls. However, algorithmic decisions may also be mistaken or discriminatory, reproducing human biases or existing biases and discriminations resulting from the combination of historical data and introducing new ones. Even when automated assessments of individuals are fair and accurate, they are not unproblematic: they may negatively affect the individuals concerned, who are subject to pervasive surveillance, persistent evaluation, insistent influence, and possible manipulation. The AI-based processing of vast masses of data on individuals and their interactions has social significance: it provides opportunities for social knowledge and better governance, but it risks leading to the extremes of 'surveillance capitalism' and 'surveillance state'.*

**e) the interlinkages between the promotion and protection of the right to privacy in the context of the use of AI and the exercise of other human rights (including the rights to health, social security, an adequate standard of living, work, freedom of assembly, freedom of expression and freedom of movement);**

*As always, a balance needs to be struck between equally fundamental human rights. This is not specific to AI-based applications, however. Right to privacy as a vehicle and prerequisite for the exercise of several human rights (including right to health, social security, freedom of expression and movement, freedom of assembly). What should be also considered is the large scale public space surveillance based on AI, and the chilling effect, among the others, on freedom of expression, assembly, movement (so, use AI for targeted searches, detection, investigations); consideration should be also given to inaccurate personal/sensitive data fed to AI systems and their impact on right to health (misdiagnosis, over-diagnosis, over-treatment etc.). Case-law from the ECHR on social security and privacy is relevant (principles fully applicable regardless of the specific context).*

**2) legislative and regulatory frameworks, including: a) information on relevant existing or proposed national and regional legislative and regulatory frameworks and oversight mechanisms;**

*At national law we are aware of a few draft laws on artificial intelligence having been presented within the Parliament and of the creation of an investigation Commission on artificial intelligence, approved by the Senate, including a cycle of hearings with experts in the field.*

*With regard to regional and international legal frameworks. the Garante, as part of the European Data Protection Board (“EDPB”), is closely following the work of the European Commission which, further to the presentation of the White Paper on “Artificial Intelligence: A European approach to excellence and trust” has led to the publication of the first Proposal for a Regulation laying down harmonised rules on artificial intelligence.*

*The Garante is also taking part in the discussion currently going on within the CAHAI, the Council of Europe Ad Hoc Committee on Artificial intelligence, whose remit is to examine the feasibility and potential elements - on the basis of broad multi-stakeholder consultations – of a legal framework, possibly an international instrument, for the development, design and application of artificial intelligence, based on Council of Europe’s standards on human rights, democracy and the rule of law.*

*The construction of a legal framework aiming at reconciling the potentiality of growth given by AI with the respect of fundamental rights and societal values should be welcome. However, the legal framework should be based on high-level and general principles, based on a precautionary approach founded on appropriate human rights risk assessment, preferably within a legally binding instrument and possibly complemented by sectoral tools. Self-regulation consistent with the general approach is also useful. However, in order to provide a substantial and efficient application of the provisions included in self-regulatory tools, it is crucial that such tools are assisted by appropriate (better if mandatory) monitoring mechanism (see below). Finally, possible new legal frameworks on AI should take fully into account the existing data protection legal framework. To provide regulatory support for the creation of such a new framework, ethical and legal principles are needed, together with sectorial regulations. The ethical principles include autonomy, prevention of harm, fairness and explicability; the legal ones include the rights and social values enshrined in the EU Charter, in the EU Treaties, as well as in national Constitutions.*

**b) analysis of related human rights protection gaps, ways to bridge those gaps and barriers to advancing effective, human-rights based regulation of AI;**

*- Difficulties in translating human rights into AI-effective principles and standards as such; learning curve of AI-based machines to be taken into account (learning by example?); risk of human-generated biases (how to prevent them?).*

*- Need for awareness-raising in developers, marketers, users (create a human-right friendly ‘environment’); poor social/collective awareness of and participation in AI-related choices (national parliaments, public debates, governmental initiatives).*

**c) assessments of the need to prohibit certain AI applications or use cases (“red lines”).**

*- This would seem of paramount importance and this is where rules are certainly needed in accordance with a top-down approach. Refer to catalogue in draft AI Regulation. Need for world-wide moratorium on certain AI uses? At least to be considered carefully, need for precautionary approach.*

*[ remote biometric identification of individuals in publicly accessible space, use of AI systems detecting emotions for the access to education, employment, etc.]*

**3) other safeguards and measures to prevent violations of privacy when using AI, and address and remedy them, where they occur, including:**

***a) self-governance approaches by business enterprises to regulate AI applications, which meet the companies' responsibilities to respect the right to privacy;***

*Recognizing that artificial intelligence systems and machine learning technologies in particular, through massive processing personal data may have direct impact on data protection, threaten privacy and other fundamental rights of individuals, when stressing the importance to put in place appropriate measures preventing violation of privacy and other fundamentals rights and freedoms of individuals should be emphasized the importance of the following safeguards:*

*a)     business enterprises should adopt self-governance approaches to regulate AI applications: the accountability of the whole chain of actors involved in design, production, delivery of AI system in this sense should be stressed;*

*b)     within those organizations should be adopted a sound internal management system that starting from assessing the risk to rights and freedom of individuals, groups, and the society at large, lead to the identification of specific technical and organizational measure such us privacy by design and by default, data anonymization, data minimization and all other necessary measure to prevent any physical, material or non-material damage to natural persons; c)     these approaches should cover all the lifecycle of AI solutions products or services continuously monitoring the quality of such AI artifacts also when delivered on the market and are adopted and used by public or private organization;*

*d)     the private and public organizations as users of AI systems should as the same conduct risk assessment to be aware of the impact on fundamental rights and freedoms of physical persons that may by threatened by the specific application and use context of AI systems, implementing appropriate safeguards and where necessary pose usage limitations;   
e)     all the relevant actors of artificial intelligence value chain, in particular when data-intensive processing of personal data occurs, should adopt data governance models granting the legitimate use, such as the quality and security of personal data on a continuous base.*

***b) human rights due diligence in the context of the use of AI by governments, business enterprises and international organizations;***

*- Yes, absolutely as part of risk assessment*

*c****) data governance models, such as data trusts, that provide effective protection to the right to privacy in data-intensive environments;***

***d) technological applications that could help adequately protect the right to privacy when applying AI and their limits****.*

*Inputs, information and analysis relating to the above issues in the context of the use of AI in the following specific areas would be particularly appreciated: surveillance by intelligence, security and law enforcement agencies (e.g., facial recognition in public spaces, predictive policing, social media monitoring); public services (e.g. health, welfare, justice); employment; delivering and filtering information online, including for content curation and moderation purposes and targeting of information; and addressing the COVID-19 pandemic.*