



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Segnalazione al Parlamento e al Governo sull'Autorità per l'i. a.



- [English version](#)

Al Presidente del Senato della Repubblica
Sen. Ignazio La Russa

Al Presidente della Camera dei Deputati
On. Lorenzo Fontana

Al Presidente del Consiglio dei Ministri
On. Giorgia Meloni

Segnalazione al Parlamento e al Governo sull'Autorità per l'i. a.

l'approvazione definitiva, lo scorso 13 marzo, del Regolamento europeo sull'intelligenza artificiale (di seguito: "Regolamento") impone adesso, agli Stati membri, alcune scelte essenziali sulle norme di adeguamento degli ordinamenti interni. Tra queste, particolare rilievo assume la designazione, ai sensi dell'art. 70 del Regolamento, della (o delle) autorità nazionali competenti per l'applicazione delle sue norme, con funzioni di vigilanza del mercato e ricezione delle notifiche previste a fini di controllo.

La stessa disposizione impone agli Stati membri di garantire che l'esercizio, da parte di tali autorità, dei propri poteri possa svolgersi "in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione" del regolamento stesso. I requisiti di indipendenza, imparzialità e assenza di pregiudizi - che secondo l'art. 70 del Regolamento devono connotare l'esercizio delle funzioni da parte delle autorità nazionali competenti per l'intelligenza artificiale (infra: i.a.) - rappresentano la diretta implicazione della dimensione "costituzionale" della disciplina europea dell'i.a.

Il suo tratto distintivo (anche rispetto a scelte di altri ordinamenti, come si evince dal raffronto con il Biden Administration's Executive Order on Artificial Intelligence) risiede, infatti, nella scelta preliminare in favore di una regolazione volta a coniugare l'innovazione con la tutela dei diritti e delle libertà fondamentali dai rischi potenzialmente derivanti da un uso scorretto dell'i.a..

Proprio quest'approccio, volto a promuovere "la diffusione di un'intelligenza artificiale antropocentrica e affidabile" (art.1, p.1) depone, dunque, per l'attribuzione di ruoli di vigilanza in materia a organi caratterizzati da sufficienti requisiti di indipendenza e terzietà. L'incidenza, profonda e trasversale, dell'i.a. sui diritti fondamentali (cui, significativamente, si rivolge la stessa valutazione d'impatto prescritta per alcuni sistemi ad alto rischio) suggerisce, infatti, di attribuirne la competenza ad Autorità caratterizzate da requisiti d'indipendenza stringenti.

In ragione della stretta interrelazione tra i.a. e protezione dati, della competenza già acquisita in materia dalle Autorità di protezione dati sul processo decisionale automatizzato (art. 22 del Regolamento UE 2016/679) e delle caratteristiche d'indipendenza che ne connotano lo statuto, sarebbe utile ragionare sulla soluzione proposta dal Comitato europeo per la protezione dati e dal Garante europeo. Con il parere congiunto n. 5 del 2021, essi hanno infatti suggerito l'individuazione, nelle Autorità di protezione dati, delle autorità di controllo per l'i.a.

Va, infatti, preliminarmente considerato che il Regolamento obbliga espressamente alla designazione delle Autorità di protezione dati quali autorità competenti rispetto all'applicazione di alcune sue disposizioni. Ai sensi dell'art. 74, p.8, infatti, "per i sistemi di IA ad alto rischio elencati nell'allegato III, punto 1, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III, punti 6, 7 e 8, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680". Inoltre, rispetto all'identificazione biometrica nell'ambito di attività di contrasto si prevede un vaglio autorizzatorio da parte di autorità giudiziarie o amministrative indipendenti (art. 5, p.3) tenute a verificare l'osservanza, tra l'altro, dei vincoli imposti dalla disciplina di protezione dati. Ciò implica, dunque, l'opportunità dell'attribuzione al Garante anche di tale funzione, in ragione della sua competenza sulle norme da applicare e delle sue caratteristiche di indipendenza.

Le Autorità di protezione dati sono, dunque, le uniche autorità effettivamente destinatarie di una riserva di competenza sancita dal Regolamento (cfr., appunto, art. 74, p.8 oltre alle varie clausole di salvaguardia in favore della protezione dati previste) e, in quanto indipendenti, legittimate a svolgere le funzioni di controllo in settori delicati come quello delle attività di contrasto (art.5, p.3). Per tale ragione, sarebbe opportuno attribuire al Garante le funzioni di cui all'art. 70 del Regolamento, ferme restando ovviamente le competenze del Governo in ordine alla generale promozione e regolazione secondaria della materia.

In termini più generali, come chiarito nel citato parere congiunto, la "designazione delle autorità per la protezione dei dati come autorità nazionali di controllo assicurerebbe (..) un approccio normativo più armonizzato e contribuirebbe all'adozione di un'interpretazione coerente delle disposizioni in materia di trattamento dei dati nonché a evitare contraddizioni nella loro applicazione nei diversi Stati membri".

Va, infatti, considerato che il controllo delle Autorità di protezione dati sui processi algoritmici che (come nella maggior parte dei casi avviene) utilizzino dati personali andrebbe comunque garantito normativamente (C 10; artt. 2, p.7; 10, p.5 e, appunto, 74, p.8) e svolto, effettivamente, nel rispetto della riserva sancita, in favore di tali Autorità, dagli artt. 8 CDFUE e 16 TFUE, con l'obbligo che ne deriva, anche al legislatore, in termini di legittimità unionale.

In assenza dell'attribuzione, al Garante, del ruolo di autorità competente in materia, infatti, andrebbero disciplinati meccanismi (non scevri da oneri amministrativi per cittadini e imprese) di coordinamento, tali da salvaguardare le competenze ascritte dai citati artt. 8 CDFUE e 16 TFUE, pena l'illegittimità della norma interna per violazione di tali parametri di diritto primario dell'Unione europea.

La designazione, quali autorità competenti per l'i.a., di organi diversi determinerebbe infatti una frammentazione eccessiva della governance, con inevitabili conflitti di competenza e duplicazione ingiustificata degli oneri amministrativi per soggetti pubblici e privati.

La soluzione auspicata garantirebbe, invece, una notevole semplificazione per gli utenti, che dovrebbero rivolgersi a un'unica autorità per i sistemi di i.a. che operino su dati personali senza il rischio di conflitti di competenza o di duplicazione di oneri amministrativi (artt. 26, p.9 e 27, p. 4),

una maggiore coerenza della disciplina - considerando che al Garante dovrebbero comunque essere riservate le competenze sui sistemi di i.a. di cui all'art. 74, p.8- nonché l'estensione, al settore dell'i.a., dello statuto di garanzie (anche in termini di indipendenza) dell'Autorità.

L'interrelazione e le reciproche implicazioni tra protezione dati e i.a. sono, infatti, tali da determinare l'esigenza costante di un'applicazione coerente dei due plessi normativi: si pensi soltanto alla biometria, per la quale il Regolamento prevede garanzie specifiche, comprensive anche del controllo sulla legittimità del trattamento dei dati personali (C 14, 38, 93, 94, 95, 159; art. 26, pp.10 e 11).

L'individuazione nel Garante dell'autorità di controllo per l'intero Regolamento (oltre, dunque, agli ambiti comunque riservatagli dall'art. 74, p.8) consentirebbe, quindi, un adeguamento tempestivo agli obblighi ivi previsti, potendo esso avvalersi dell'esperienza già maturata rispetto a quell'aspetto così dirimente dell'i.a. che è rappresentato dal processo decisionale automatizzato.

Il Garante possiede infatti, già oggi, i requisiti di competenza e, assieme, indipendenza necessari per garantire un'attuazione del Regolamento coerente con l'obiettivo di garanzia di un livello elevato di tutela dei diritti fondamentali nel ricorso all'i.a., sancito dall'art. 1, p.1.

E', del resto, significativo che lo stesso art. 74, p.9, del Regolamento designi il Garante europeo per la protezione dei dati quale autorità competente, in ambito UE.

Non si può, dunque, che suggerire- come già fatto in varie audizioni parlamentari- una riflessione su questo aspetto, nella consapevolezza di quanto la sinergia tra le due discipline - e, quindi, la loro applicazione da parte di un'unica Autorità- sia determinante per l'effettività dei diritti e delle garanzie che sanciscono, con significativa lungimiranza.

Si tratta, complessivamente, di profili meritevoli di un ulteriore approfondimento che segnalo, ai sensi dell'articolo 57, paragrafo 1, lett. c), del Regolamento (UE) 2016/679, in vista dell'adozione delle norme di adeguamento al Regolamento grato, anche a nome del Collegio del Garante, per l'attenzione che vorrà riservarvi, con la più ampia disponibilità dell'Autorità, che sin d'ora Le rappresento, a ogni collaborazione eventualmente ritenuta utile.

Pasquale Stanzone



To the President of the Senate of the Republic
Ignazio La Russa

To the President of the Chamber of Deputies
Lorenzo Fontana

To the President of the Council of Ministers
Giorgia Meloni

The final approval on 13 March of the EU Artificial Intelligence Act (hereinafter: "Act") now requires Member States to make a number of essential choices regarding the rules for the adaptation of their domestic legislation. Particularly important among these is the designation, pursuant to Article 70 of the Act, of the National Authority (or Authorities) responsible for the application of the provisions contained in the Act itself, having market surveillance functions and receiving notifications for control purposes.

The same provision requires Member States to ensure that these authorities exercise their powers “independently, impartially and without bias, so as to safeguard the principles of objectivity of their activities and tasks and to ensure the application and enforcement” of the Act itself. The requirements of independence, impartiality and absence of bias - which, according to Article 70 of the Act, shall govern the manner in which the national authorities competent for artificial intelligence (hereinafter: A.I.) exercise their functions - directly reflect the ‘constitutional’ dimension of the European AI Act.

Its distinctive feature (also with respect to choices made by other jurisdictions, as can be seen by comparing it with the Biden Administration's Executive Order on Artificial Intelligence) lies, in fact, in the preliminary choice to favour a regulation aimed at combining innovation with the protection of fundamental rights and freedoms from the risks that could potentially derive from an improper use of A.I.

It is precisely this approach, aimed at promoting “the diffusion of an anthropocentric and reliable artificial intelligence” (Art.1, paragraph 1), which advocates, therefore, the attribution of supervisory roles in the matter to bodies characterised by the necessary requisites of independence and impartiality. The profound and extensive impact of A.I. on fundamental rights (which requires the same impact assessment prescribed for some high-risk systems is addressed) suggests, in fact, that the matter be entrusted to Authorities with stringent independence requirements.

In view of the close interrelation between A.I. and data protection, of the expertise already acquired in the field by the DPAs on automated decision-making (Article 22 of EU Regulation 2016/679), and of the independent nature that characterises their statute, it might be useful to consider the solution proposed by the European Data Protection Board and the European Data Protection Supervisor. In their Joint Opinion No. 5 of 2021, they in fact suggested identifying DPAs as the supervisory authorities for A.I.

In fact, it should first be considered that the Act expressly requires the designation of DPAs as competent authorities with respect to the application of a number of its provisions. According to Article 74, paragraph 8, in fact, “for the high-risk AI systems listed in Annex III, point 1, insofar as such systems are used for law enforcement, border management, justice and democracy purposes, and for the high-risk AI systems listed in Annex III, points 6, 7 and 8, Member States shall designate as market surveillance authorities for the purposes of this Act the competent data protection authorities in accordance with Regulation (EU) 2016/679 or Directive (EU) 2016/680”. Furthermore, with respect to biometric identification in the context of law enforcement activities, an authorisation check is envisaged by independent judicial or administrative authorities (Art. 5, paragraph 3), which are required to verify compliance with, inter alia, the constraints imposed by data protection regulations. This therefore suggests that the Garante should also be entrusted with this function, on account of its competence over the rules to be applied and of its independent nature.

The Data Protection Authorities are, therefore, the only authorities to have actually been provided with jurisdiction by the Act (see Art. 74, paragraph 8, in addition to the various safeguard clauses in favour of data protection provided for) and, as independent, legitimated to perform the control functions in sensitive sectors such as law enforcement (Art. 5 paragraph 3). For this reason, it would be appropriate that the Garante be assigned the functions referred to in Article 70 of the Act, without prejudice, of course, to the Government's powers as regards the general promotion and secondary regulation of the matter.

In more general terms, as clarified in the aforementioned joint opinion, the “designation of the data protection authorities as national supervisory authorities would ensure (...) a more harmonised regulatory approach and contribute to the adoption of a consistent interpretation of the provisions

on data processing, as well as to avoid contradictions in their application in the different Member States”.

In fact, it should be considered that the control of the Data Protection Authorities over algorithmic processes that (as in most cases) use personal data should in any case be guaranteed by law (recital 10; art. 2, paragraph 7; art. 10, paragraph 5 and, precisely, art.74, paragraph 8) and carried out, in fact, in compliance with the legal provision set forth, in favour of such Authorities, by article 8 of the EU Charter of Fundamental Rights and article 16 of the Treaty on the Functioning of the European Union, with the obligation that derives from it, also to the legislator, in terms of EU legitimacy.

Should the Garante not be assigned the role of competent authority in the matter, in fact, coordination mechanisms (not free from administrative burdens for citizens and businesses) should be regulated, such as to safeguard the competences ascribed to it by the aforementioned article 8 of the CFR and article 16 of the TFEU, under penalty of the unlawfulness of the internal rule for breach of such parameters of primary European Union law.

The designation of different bodies as competent authorities for A.I. would in fact lead to an excessive fragmentation of governance, with inevitable conflicts of competence and unjustified duplication of administrative burdens for public and private entities.

The desired solution would, on the other hand, ensure considerable simplification for users, who would have to refer to a single authority for A.I. systems operating on personal data without the risk of conflicts of competence or duplication of administrative burdens (article 26, paragraph 9 and article 27 paragraph 4), a greater consistency of the rules - considering that the Garante should in any case be reserved the competences on A.I. systems under article 74 paragraph 8 - as well as the extension of the Authority's status of guarantees (also in terms of independence) to the A.I. sector.

The interrelation and reciprocal implications between data protection and A.I. are, in fact, such as to determine the constant need for a consistent application of the two sets of rules: just think of biometrics, for which the Act provides for specific guarantees, including the control of the lawfulness of the processing of personal data (recital 14, 38, 93, 94, 95, 159; art. 26, paragraphs 10 and 11).

Identifying the Garante as the supervisory authority for the entire Act (in addition, therefore, to the areas reserved to it by article 74, paragraph 8) would therefore allow it to promptly adapt to the obligations laid down therein, since it could draw on the experience it has already gained in respect of that aspect of A.I. that is so crucial, namely automated decision-making.

As a matter of fact, the Garante already possesses the requirements of competence and, at the same time, independence necessary to ensure an implementation of the Act consistent with the objective of guaranteeing a high level of protection of fundamental rights in the use of the A.I., as set out in Article 1, paragraph 1.

It is, moreover, significant that Article 74, paragraph 9 of the Act itself designates the European Data Protection Supervisor as the competent authority within the EU.

Therefore, it is only right to suggest - as has already been done in various parliamentary hearings - a reflection on this aspect, in the awareness of how much the synergy between the two disciplines - and, therefore, their application by a single Authority - is crucial for ensuring the effectiveness of the rights and guarantees they set forth, with significant foresight.

Overall, these aspects deserve further in-depth analysis, and I would like to draw your attention to them, pursuant to Article 57, paragraph 1, letter c) of Regulation (EU) 2016/679, in view of the

adoption of the rules to comply with the Act. I am grateful, also on behalf of the Garante Supervisory Board, for the attention you will want to reserve it. The Garante, which I represent, remains at your disposal for any cooperation deemed useful.

Pasquale Stanzione