RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 2-2022
DOI: 10.32091/RIID0086
Articolo sottoposto a peer review

La gestione del rischio informatico nella decisione amministrativa robotica

Luigi Previti

Il presente contributo mira ad analizzare uno dei principali rischi connessi all'avanzamento del processo di algoritmizzazione delle decisioni amministrative, ossia quello relativo alla tutela della sicurezza informatica. Nello specifico, dopo aver ricostruito l'articolato sistema multilivello definito negli ultimi anni in materia di cybersicurezza, l'indagine evidenzia la necessità di assicurare un livello adeguato di resilienza cibernetica in sede di automazione delle diverse procedure amministrative, formulando alcune considerazioni finali in merito alla stessa legittimità del ricorso alle formule algoritmiche ai fini decisionali.

Intelligenza artificiale – Decisioni amministrative robotiche – Cybersicurezza – Rischio informatico

Sommario: *1. Decisioni amministrative ai tempi della Società del rischio tecnologico – 2. Le sfide della cibernetica per l'azione amministrativa – 3. La sfida più importante (e spesso dimenticata): pubblico e privato di fronte alle trappole della rete informatica – 4. Verso una pubblica amministrazione "security by design"*

1. Decisioni amministrative ai tempi della Società del rischio tecnologico

Negli ultimi anni dottrina e giurisprudenza sono tornate ad interrogarsi in merito alle sfide, concettuali e operative, poste dall'avanzamento del processo di digitalizzazione dell'azione amministrativa.

Nell'attuale contesto economico e sociale, fortemente condizionato dall'avvento della "Società del rischio" e della "Società Algoritmica", l'uso delle tecnologie informatiche non incide più, infatti, sulle sole modalità di comunicazione tra pubblico e privato o sulle modalità di gestione dei singoli procedimenti, ma si riverbera direttamente sulle modalità con le quali le pubbliche amministrazioni adottano le proprie decisioni e orientano le proprie attività istituzionali nei confronti degli amministrati[1].

In considerazione delle significative opportunità offerte dall'utilizzo delle formule algoritmiche nella cura degli interessi pubblici si è assistito, di conseguenza, a numerosi tentativi di inquadramento teorico e di adeguamento interpretativo del fenomeno, con l'obiettivo di ricondurre anche le tecnologie più sofisticate alle regole e ai principi che connotano l'agire procedimentale dei pubblici poteri[2].

Tuttavia, accanto al crescente interessamento, a livello nazionale ed europeo, per le possibili applicazioni dei sistemi di intelligenza artificiale nel settore pubblico, un analogo interesse non pare essere stato mostrato, se non da ultimo, nei confronti della dimensione organizzativa e, più in particolare, nei confronti delle rilevanti problematiche legate alla salvaguardia della pubblica sicurezza cibernetica (o c.d. cybersicurezza).

Fino ad ora gli ordinamenti giuridici moderni hanno assicurato un livello minimo di sicurezza collettiva attraverso la codificazione di un sistema istituzionale fortemente radicato su categorie e principi chiari e definiti, quali il primato della legge come garanzia dei

---

L. Previti è ricercatore a tempo determinato di Diritto amministrativo presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Palermo. Questo saggio fa parte della sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura di Benedetto Ponti.

diritti individuali, la spazialità dell'applicazione delle norme giuridiche, il ricorso a meccanismi di prevenzione e di contrasto alla criminalità che si fondano sull'intervento degli apparati delle Forze dell'ordine. Queste coordinate concettuali rischiano, tuttavia, di non essere più adatte ad affrontare le criticità derivanti dalla diffusione della nuova dimensione cibernetica, all'interno della quale vengono rimesse in discussione sia l'applicazione degli istituti giuridici consolidati sia il ruolo tradizionalmente esercitato dai diversi organi politici e burocratici.

Pur mantenendo una prospettiva di indagine assiologicamente neutrale, il presente contributo mira dunque ad evidenziare uno dei principali rischi connessi al repentino sviluppo del processo di robotizzazione delle attività amministrative[3], ossia quello relativo alla tutela della sicurezza cibernetica.

In particolare, dopo aver rimarcato il carattere ontologicamente rischioso di ogni operazione procedurale condotta tramite sistemi informatici, verranno analizzate, seppur brevemente, le caratteristiche e l'articolazione dell'attuale architettura multilivello in materia di cybersicurezza, con l'obiettivo di trarre, a margine di tale indagine, alcune implicazioni sistematiche in ordine alla stessa legittimità del ricorso all'automazione decisionale all'interno del nostro ordinamento.

2. Le sfide della cibernetica per l'azione amministrativa

La progressiva ingegnerizzazione delle funzioni amministrative ha reso non ulteriormente procrastinabile l'esigenza di implementare un sistema istituzionale in grado di individuare e gestire le peculiari incertezze e criticità che tale fenomeno inevitabilmente comporta.

Anche le riflessioni dottrinali che da ultimo si sono occupate di indagare l'ammissibilità e le modalità di utilizzo dei diversi sistemi di intelligenza artificiale all'interno del settore pubblico sembrano ormai concordare sull'impossibilità di sfruttare a pieno i vantaggi derivanti dalla crescente informatizzazione dell'azione amministrativa prescindendo dall'analisi del grado e della tipologia dei rischi riconducibili alle nuove tecnologie[4].

Uno dei rischi più evidenti in materia è certamente quello relativo all'opacità dell'*iter* decisionale seguito dalle pubbliche amministrazioni[5].

Com'è noto, infatti, le moderne tecnologie non possono essere assimilate a quelle in uso nei primi anni degli anni '90, dal momento che queste non si limitano più ad attuare pedissequamente le specifiche istruzioni elaborate dal programmatore, ma sono dotate della capacità di definire, a loro volta, percorsi decisionali talora non prevedibili e non verificabili *a posteriori*.

Sicché, se neppure colui che ha fornito le istruzioni è pienamente in grado di ripercorrere il procedimento logico-matematico seguito dal software e offrire una ragionevole spiegazione della decisione adottata, la preoccupazione maggiormente avvertita è quella di costruire un modello di pubblica amministrazione che si caratterizza per essere, da un lato, più moderna ed efficiente, ma, dall'altro, più oscura e imperscrutabile.

Una circostanza in grado di riflettersi, a ben vedere, anche sullo stesso ruolo del funzionario amministrativo chiamato ad adottare il provvedimento finale, il quale potrebbe assumere, nel nuovo contesto digitalizzato, una funzione più formale e rappresentativa rispetto al passato, laddove il ruolo di decisore sostanziale (seppur "invisibile") verrebbe sostanzialmente affidato all'elaboratore elettronico.

Accanto al rischio di opacità o di invisibilità dell'amministrazione algoritmica, la dottrina ha più volte evidenziato il rischio di pervenire ad esiti discriminatori[6].

Ogni processo di automazione richiede, in primo luogo, l'esecuzione di un'operazione di traduzione delle istruzioni redatte in linguaggio umano (ossia, i criteri di valutazione, i riferimenti normativi, i passaggi logici, ecc.) in un linguaggio tecnico, comprensibile per la macchina.

Tale operazione non costituisce, tuttavia, un'attività di natura meccanica, ma rappresenta, invece, un momento procedurale estremamente delicato, nel quale è ben possibile che si verifichino traduzioni semantiche infedeli, imprecise o errate, in grado di condurre all'adozione di decisioni finali irragionevoli e/o discriminatorie.

Allo stesso tempo, è ben possibile che la violazione del principio di non discriminazione si realizzi per la scarsa qualità dei dati acquisiti dal software. Una circostanza che conduce a riflettere sulla necessità di garantire, quantomeno in alcuni casi, appositi momenti di controllo degli esiti procedurali raggiunti dalla macchina, al fine di verificare che le regole di funzionamento della procedura automatizzata definite *ex ante* siano rispettate prima dell'adozione del provvedimento amministrativo.

A ciò si aggiunga che il rischio di ottenere una decisione amministrativa contraria al principio di non discriminazione è molto più elevato qualora vengano adoperati algoritmi di tipo non deterministico. È in queste ipotesi, infatti, che è necessario richiedere all'amministrazione procedente di svolgere un controllo più penetrante e costante, dal momento che, in tali fattispecie, non è sempre possibile garantire che il risultato della procedura automatizzata sia in linea con le finalità e i criteri di giudizio definiti in sede di progettazione.

Più di recente, il tema della gestione del rischio legato all'utilizzo di sistemi e procedure informatizzate è stato oggetto di specifica attenzione a livello sovranazionale, come si evince dalla recente proposta di regolamento europeo sull'intelligenza artificiale, pubblicata dalla Commissione europea il 21 aprile 2021[7].

Con tale atto è stata suggerita, per la prima volta, l'introduzione di un quadro omogeneo di condizioni e di requisiti minimi ispirati ad una logica di tipo *risk-based*, ossia parametrati allo specifico livello di rischio che i singoli sistemi informatici presentano nei confronti della sicurezza, della salute e della sfera giuridica individuale. Un approccio metodologico che si fonda, in particolare, sulla fissazione di limitazioni d'uso e di obblighi di progettazione chiari e proporzionati, sul contenimento dei costi di conformità alla normativa di settore da parte degli operatori economici e sulla previsione di oneri di monitoraggio e di segnalazione degli incidenti in capo agli stessi utenti.

Se è dunque chiaro che un uso irragionevole e indisciplinato della tecnologia può rappresentare un grave e serio rischio per i diritti e le libertà fondamentali, diviene sempre più pressante l'esigenza di monitorare e salvaguardare il livello di sicurezza cibernetica raggiunto a livello nazionale, quale strumento centrale per prevenire e contrastare il diffondersi di indebite intrusioni, manomissioni e alterazioni ad opera dei sempre più pericolosi criminali informatici.

3. La sfida più importante (e spesso dimenticata): pubblico e privato di fronte alle trappole della rete informatica

L'obiettivo di tutelare la sicurezza delle reti e dei dispositivi elettronici viene espressamente menzionato negli atti di indirizzo di livello europeo quantomeno a partire dai primi anni del XXI secolo, ove si rimarca la circostanza secondo la quale la cybersicurezza rappresenta la naturale precondizione per la crescita e lo sviluppo sostenibile degli Stati tecnologicamente avanzati[8].

Tuttavia, la necessità di assicurare un livello più elevato di protezione dei diritti degli operatori pubblici e privati che utilizzano, per diverse finalità, le moderne tecnologie ha condotto solo negli ultimi anni le istituzioni dell'Unione ad adottare un quadro normativo maggiormente chiaro e definito.

Sotto questa prospettiva, l'interesse del legislatore per la predisposizione di un apparato pubblicistico di contrasto nei confronti delle minacce cibernetiche rappresenta il necessario contraltare rispetto all'impulso verso lo sviluppo e la diffusione di applicazioni informatiche sempre più sofisticate e interconnesse[9].

Al riguardo occorre osservare come la definizione di una solida ed efficace strategia in materia di cybersicurezza sia strettamente correlata alle politiche europee di implementazione del mercato unico digitale, all'interno del quale si intende garantire non solo un'ampia offerta di servizi digitali personalizzati, ma anche un soddisfacente grado di resilienza contro il rischio di attacchi cibernetici[10].

Il raggiungimento di tale finalità ispira chiaramente la direttiva UE 2016/1148, nota anche come "direttiva NIS" (*Network and Information Security*), che rappresenta il primo importante tentativo di armonizzazione delle legislazioni nazionali in tema di sicurezza informatica[11].

Nello specifico, la direttiva ha stabilito una serie di rilevanti misure tecniche ed organizzative per due determinate categorie di soggetti, ossia i c.d. "operatori dei servizi essenziali" (OSE) e i "fornitori di servizi digitali" (FSD), la cui intensità è direttamente proporzionale alla strategicità e alle dimensioni dei singoli destinatari[12].

Si tratta di obblighi principalmente rivolti a rendere più affidabili le reti utilizzate dai predetti soggetti, a prevedere e minimizzare l'impatto delle minacce più significative sulla continuità delle operazioni e dei servizi svolti, nonché ad assicurare la tempestiva comunicazione degli incidenti di sicurezza alle competenti autorità nazionali NIS.

Più di recente, il legislatore europeo è intervenuto per rivedere e aggiornare le linee strategiche e operative precedentemente stabilite[13]. Una decisione sulla quale hanno certamente influito sia la consapevolezza dell'intensificarsi e dell'evoluzione delle minacce cibernetiche a livello globale[14], sia l'intenzione di affermare una più chiara visione europea del cyberspazio[15].

In questo senso vanno lette le disposizioni introdotte dal regolamento UE 2019/881, c.d. *Cybersecurity Act*[16], il quale si caratterizza per la previsione di due significativi interventi: il primo riguarda l'istituzione di un sistema europeo di certificazione della cybersicurezza, ossia un insieme di regole e procedure volte ad assicurare, all'interno del territorio dell'Unione, la conformità di prodotti, servizi e processi ICT rispetto a determinati parametri minimi di sicurezza informatica; il secondo riguarda il rafforzamento dei poteri istituzionali dell'Agenzia europea per la cybersicurezza (*European Union Agency for Network and Information Security*, di seguito ENISA), autorità istituita nel 2004 con lo scopo di assistere le istituzioni europee e gli Stati membri nello sviluppo e nella revisione delle politiche e delle azioni strategiche in materia.

Nell'ambito del nuovo mandato, viene così attribuito all'Agenzia il compito di fornire pareri, consulenze e orientamenti, sostenere lo scambio di informazioni e di buone pratiche, promuovere il miglioramento delle tecniche di prevenzione, analisi e reazione nei confronti delle minacce più pericolose, stimolare l'aggiornamento della normativa europea di settore, supportare la rete europea dei CSIRT, incentivare l'uso del citato meccanismo di certificazione dei prodotti e dei servizi ICT e sensibilizzare l'opinione pubblica sui rischi informatici attualmente più diffusi. Si tratta, a ben vedere, di iniziative che perseguono chiari obiettivi di cooperazione interistituzionale, di coordinamento operativo e di incremento qualitativo delle misure organizzative, nonché di risposta alle situazioni di crisi di portata transfrontaliera aventi ad oggetto settori nevralgici dell'economia[17].

Volgendo lo sguardo al livello nazionale, è possibile osservare come la costruzione di un apposito sistema istituzionale di gestione dei rischi derivanti dal crescente aumento delle minacce informatiche sia stata affidata, in un primo momento, a fonti normative di rango non primario, attraverso le quali si è realizzato il coordinamento di corpi amministrativi preesistenti, principalmente attivi nel «Sistema di informazione per la sicurezza della Repubblica» di cui alla l. 3 agosto 2007, n. 124.

All'interno di tale contesto, un ruolo di cruciale importanza viene affidato al Presidente del Consiglio dei ministri, nella qualità di vertice del citato Sistema di informazione per la sicurezza, al quale è attribuita la definizione degli indirizzi e degli obiettivi generali della politica di sicurezza cibernetica. Tale funzione trova concreta manifestazione, segnatamente, nell'elaborazione di direttive[18] e di documenti programmatici, come il Quadro strategico nazionale e il Piano nazionale per la protezione cibernetica e la sicurezza informatica, che mirano a rafforzare la protezione delle infrastrutture critiche, materiali e immateriali, presenti sul territorio[19].

L'attuazione degli indirizzi e degli obiettivi fissati nei suddetti atti viene devoluta, invece, a una pluralità di organismi di supporto e di coordinamento operativo, tra i quali occupano una posizione di rilievo: il Comitato interministeriale per la sicurezza della Repubblica - CISR, con funzioni di consulenza rispetto agli atti di indirizzo di competenza del Presidente del Consiglio e di proposta rispetto alle misure normative e organizzative ritenute necessarie[20]; il Dipartimento delle informazioni per la sicurezza della Repubblica (di seguito, DIS), incaricato di presiedere tutte le attività di ricerca, di analisi e di elaborazione informativa relative alle minacce e agli attacchi cibernetici[21]; il Nucleo per la Sicurezza Cibernetica, istituito dal d.P.C.M. n. 66/2013 al fine di coordinare l'azione di tutti i soggetti coinvolti nella preparazione e nella gestione delle situazioni di crisi e di attivare le eventuali procedure di allerta e di risposta[22].

Seppur improntato ad un principio di razionale distribuzione delle funzioni tra i diversi attori istituzionali, il disegno normativo sopra descritto, tuttavia, si è rivelato presto alquanto complesso e inefficiente.

A tali lacune cercano di porre rimedio il successivo d.P.C.M. 17 febbraio 2017[23], nonché, in aderenza alle sollecitazioni europee, il d.lgs. 18 maggio 2018, n. 65, che recepisce la ricordata direttiva NIS, il d.l. 21 settembre 2019, n. 105, convertito dalla l. 18 novembre 2019, n. 133, che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica - PSNC[24] e il d.l. 14 giugno 2021, n. 82, convertito dalla l. 4 agosto 2021, n. 109, che ha istituito, con colpevole ritardo rispetto alle esperienze di altri Paesi, l'Agenzia per la cybersicurezza nazionale.

Alla predetta autorità il d.l. n. 82/2021 ha affidato compiti e responsabilità peculiari, che riguardano, principalmente, la prevenzione e la tutela della sicurezza nazionale nel cyberspazio, l'ispezione, l'accertamento e l'irrogazione delle sanzioni prescritte in caso di violazione della normativa di settore, la gestione delle vulnerabilità informatiche e le attività di contrasto in caso di attacco[25].

Nell'ambito di queste ultime attività, funzioni di grande rilevanza sono attribuite al CSIRT Italia, introdotto in sede di recepimento della direttiva NIS e incardinato, dapprima, presso il DIS e, oggi, trasferito presso l'Agenzia[26]. Spetta al predetto gruppo di intervento, in particolare, monitorare periodicamente il verificarsi di attacchi e di incidenti a livello nazionale, ricevere le segnalazioni obbligatorie provenienti dagli OSE e dai FSD di cui alla direttiva NIS e le segnalazioni facoltative provenienti dagli altri soggetti, pubblici e privati, comunque interessati da una minaccia *cyber*, emettere preallarmi e allerte e offrire assistenza operativa in situazioni di crisi.

All'Agenzia nazionale spettano, inoltre, importanti compiti di promozione e di coordinamento delle iniziative e dei progetti rivolti alla formazione e alla sensibilizzazione collettiva sulle problematiche riguardanti la cybersicurezza. Attività che vengono espletate sia tramite il supporto di un organo interno, ossia il Comitato tecnico-scientifico, sia tramite il coinvolgimento delle università, degli enti di ricerca, del sistema produttivo nazionale e delle altre istituzioni pubbliche competenti.

L'istituzione dell'autorità, che opera quale interlocutore unico per i soggetti ricompresi nel PSNC, pare conferire maggiore compattezza ad un disegno normativo inizialmente frammentato e complesso, che

risulta oggi improntato all'accentramento delle competenze e al coordinamento delle linee strategiche e delle azioni operative, nell'ottica della semplificazione delle procedure decisionali e dell'eliminazione delle preesistenti sovrapposizioni funzionali[27].

Le suddette scelte di governance, per quanto aderenti alle indicazioni di matrice europea, paiono riflettere, invero, l'intenzione del legislatore nazionale di salvaguardare le sole infrastrutture strategiche per la vita economica e sociale del Paese, laddove sarebbe stato più opportuno estendere la copertura assicurata dall'architettura istituzionale nei confronti di soggetti ed enti di rilevanza nazionale, sebbene non rientranti nel menzionato PSNC.

4. Verso una pubblica amministrazione "security by design"

L'analisi del sistema multilivello congegnato in materia di cybersicurezza consente di svolgere alcune considerazioni finali in merito alle attuali esigenze di prevenzione e di contrasto nei confronti dei sempre più frequenti attacchi informatici all'interno del settore pubblico.

A tal proposito alcune interessanti indicazioni parrebbero potersi trarre dai recenti principi affermati *in subiecta materia* a livello sovranazionale[28].

Da un lato, assume rilevanza il c.d. principio di "sicurezza *by design*", in base al quale i produttori e i fornitori devono immettere sul mercato unicamente beni e/o servizi in grado di assicurare determinati livelli di resilienza contro il rischio di incidenti e attacchi. Un'obbligazione, quest'ultima, che non solo deve essere rispettata fin dal momento della progettazione dell'infrastruttura o del dispositivo, ma che costituisce altresì una specifica parte della prestazione contrattuale assunta dal professionista nei confronti del consumatore[29].

Dall'altro, merita di essere richiamato il c.d. "principio di responsabilità", in virtù del quale gli operatori economici del settore devono assumere, nei confronti degli utenti della rete, il ruolo di interlocutori privilegiati durante l'intero ciclo di vita dei prodotti ICT acquistati sul mercato. Una circostanza che determina per tali soggetti il sorgere di un particolare dovere di diligenza, che si esplica, ad esempio, nell'obbligo di curare i necessari aggiornamenti software dei prodotti, di risolvere con celerità le vulnerabilità segnalate dai consumatori, nonché di garantire un corretto utilizzo dei dati personali trattati nello svolgimento delle proprie attività imprenditoriali[30].

In altri termini, secondo la moderna visione europea di cyberspazio, tutte le imprese che intendono offrire i propri prodotti online hanno l'obbligo di mantenere e preservare un soddisfacente livello di sicurezza delle reti e dei sistemi informatici utilizzati, assumendosi la responsabilità di ogni eventuale danno o pregiudizio cagionato a terzi in ragione dell'inadempimento della suddetta obbligazione.

Declinando le suddette indicazioni all'interno dello specifico contesto dell'automazione delle procedure amministrative, non parrebbe irragionevole pretendere, oltre a quelle garanzie procedimentali fissate dall'ormai nota giurisprudenza amministrativa[31], anche il rigoroso rispetto, fin dalla progettazione (*by design*), di un adeguato livello di *cyber*-resilienza per le piattaforme, i dispositivi e i dati utilizzati dalla pubblica amministrazione.

Seguendo tale ragionamento, in particolare, sarebbe possibile giungere ad elevare la sicurezza dei software e delle reti informatiche coinvolti nei processi di automazione in un ulteriore requisito minimo di legittimità delle decisioni amministrative robotiche, la cui mancanza ben potrebbe essere censurata in sede giurisdizionale, con tutte le conseguenze sul piano risarcitorio che da ciò potrebbero discendere.

Si auspica, pertanto, una futura adesione giurisprudenziale ad una siffatta impostazione, la quale pare poter concorrere effettivamente all'accrescimento del senso di fiducia dei cittadini nei confronti dell'intelligenza artificiale e delle sue applicazioni, nonché alla realizzazione di una visione autenticamente antropocentrica del processo di algoritmizzazione delle procedure amministrative.

Note

[1]Sul concetto di "Società dell'Algoritmo", è doveroso il rinvio a J.M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in "Ohio State Law Journal", 2017, n. 78, p. 1219, secondo il quale la predetta locuzione identificherebbe «a society organized around social and economic decision-making by algorithms, robots, and AI agents, who not only make the decisions but also, in some cases, carry them out». Sui rischi connessi alla diffusione del c.d. "ignoto tecnologico", si veda, invece, il lavoro di A. Barone, *Il diritto del rischio*, Giuffrè, 2006, *passim*. Più in generale, sulla possibilità di qualificare la società contemporanea come "Società del rischio", si vedano, per tutti, U. Beck, *La società del rischio. Verso una seconda modernità*, Carocci, 2000, spec. p. 25 ss., ove l'A. sottolinea che «nella modernità avanzata la produzione sociale di ricchezza va sistematicamente di pari passo con la produzione sociale di rischi» e, in particolare, quelli «prodotti dalla scienza e dalla tecnica», nonché F. Fukuyama, *L'uomo oltre l'uomo. Le conseguenze della rivoluzione biotecnologica*, Mondadori, 2002.

[2]Per una ricostruzione analitica delle diverse posizioni dottrinali e giurisprudenziali affermatesi nel tempo *in subiecta materia* sia consentito rinviare a L. Previti, *La decisione amministrativa robotica*, Editoriale Scientifica, 2022.

[3]Come ricorda A. Santosuosso, *Diritto, scienza, nuove tecnologie*, Cedam, 2016, p. 323, il termine "robot", di origine ceca, significa letteralmente "lavoro duro/pesante" ed è stato coniato, per la prima volta, dal drammaturgo Karel Capek,

negli anni '20 del XX secolo, per riferirsi ad umanoidi adibiti al lavoro di schiavi, creati dall'uomo con il precipuo scopo di sollevarlo dalla fatica fisica. Con l'espressione "decisione amministrativa robotica" ci si riferisce, dunque, a quelle decisioni assunte dalle pubbliche amministrazioni attraverso il ricorso ad appositi sistemi informatici, ossia a quell'istituto che parte della dottrina etichetta talora con le espressioni "decisione amministrativa automatizzata" e "decisione amministrativa algoritmica" (locuzioni, quest'ultime, invero alquanto generiche, in considerazione della diversità, oltre che dei livelli di automazione decisionale, delle tipologie di formule algoritmiche attualmente esistenti).

[4]In materia, cfr. ancora A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in "European Review of Digital Administration Law", 2020, n. 1-2, p. 65 ss., secondo il quale l'intera tematica dell'IA è dominata dalle esigenze di regolazione e di gestione dei rischi (sociali, economici, tecnici) che possono derivare dall'uso delle nuove tecnologie.

[5]In materia, cfr. J. Barrat, *Our Final Invention: Artificial intelligence and the End of the Human Era*, Thomas Dunne Books, 2013; F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015; C. Coglianese, D. Lehr, *Regulating by Robot. Administrative Decision Making in the Machine-Learning Era*, in "Georgetown Law Journal", 2017, n. 105, *passim*; B.D. Mittelstadt, P. Allo, L. Floridi et al., *The ethics of algorithms. Mapping the debate*, in "Big data & Society", 2016, n. 21, p. 3 ss.; A. Cerrillo i Martínez, *How can we open the black box of public administration? Transparency and accountability in the use of algorithms*, in "Revista Catalana de Dret Públic", 2019, n. 58, p. 15 ss.

[6]Sui rischi di discriminazione riconducibili all'utilizzo di meccanismi decisionali robotici, si vedano, *ex multis*, F. Costantino, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in "Diritto pubblico", 2019, n. 1, p. 56 ss.; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal", 2019, n. 1, p. 84 ss.; F. De Leonardis, *Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione*, in E. Calzolaio (a cura di), "La decisione nel prisma dell'intelligenza artificiale", Cedam, 2020, p. 152 ss.; M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in "federalismi.it", 2019, n. 16, p. 19; G. Pesce, *Il Consiglio di Stato ed il vizio dell'opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, in "www.giustizia-amministrativa.it", 16 gennaio 2020, p. 12 ss.; P. Savona, *Administrative Decision-Making after the Big Data Revolution*, in "federalismi.it", 2018, n. 19, p. 22 ss.

[7]Cfr. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, COM(2021) 206 final. In materia si vedano, quantomeno, G. Marchianò, *Proposta di regolamento della Commissione europea del 21 aprile 2021 sull'intelligenza artificiale con particolare riferimento alle IA ad alto rischio*, in "Ambientediritto.it", 2021, n. 2; C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in "BioLaw Journal", 2021, n. 3, p. 415 ss.; G. De Gregorio, F. Paolucci, O. Pollicino, *L'intelligenza artificiale made in UE è davvero "umano-centrica"? I conflitti della proposta*, in "Agendadigitale.eu", 22 luglio 2021; F. Lamberti, *La proposta di regolamento UE sull'Intelligenza artificiale alla prova della privacy*, in "federalismi.it", 29 giugno 2022.

[8]Tra i primi interventi normativi in materia si vedano: la comunicazione della Commissione europea del 6 giugno 2001, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM(2001) 298, par. 2.1, in base alla quale: «La sicurezza delle reti e dell'informazione va intesa come la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema»; la direttiva 2002/21/CE del 7 marzo 2022, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica e affida alle autorità nazionali di regolazione il compito di garantire il mantenimento dell'integrità e della sicurezza delle reti e delle comunicazioni pubbliche (art. 8, co. 4, lett. f); la comunicazione della Commissione europea del 26 settembre 2003, *Il ruolo dell'e-Government per il futuro dell'Europa*, COM(2003) 567, par. 2.1, ove si riconosce che: «In futuro i cittadini esigeranno sempre più che le pubbliche autorità provvedano a tutelare la libertà, la giustizia e la sicurezza in tutta l'Unione europea. Occorre a tal fine garantire una cooperazione tra gli Stati membri e a livello internazionale e fare anche fronte a nuove forme di insicurezza generate dall'utilizzo di nuove tecnologie».

[9]Com'è noto, si assiste oggi ad una moltiplicazione di sistemi e dispositivi costantemente connessi ad internet, in grado di interagire tra di loro e con il mondo fisico attraverso l'uso di appositi sensori, plasmando in tal modo una rete di strumenti informatici ormai nota con l'espressione *Internet of Things* - IoT. Sul punto, cfr. R.H. Weber, E. Studer, *Cybersecurity and the Internet of Things: Legal Aspect*, in "Computer Law & Security Review", 2016, n. 36, p. 726 ss.; A. Rayes, S. Salam, *Internet of Things: from Hype to Reality*, Springer, 2019; L. De Nardis, *The Internet in Everything. Freedom and Security in a World with No Off Switch*, Yale University Press, 2020; G. Noto La Diega, *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies*, Routledge, 2022.

[10]Comunicazione della Commissione europea del 6 maggio 2015, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final. Sul punto, cfr. anche il regolamento UE 2021/694 del 29 aprile 2021 che istituisce il Programma "Europa digitale" (2021-2027): «La fiducia costituisce una condizione essenziale per il funzionamento del mercato unico digitale. Le tecnologie della cybersicurezza, come le identità digitali, la crittografia e il rilevamento delle intrusioni, e le loro applicazioni in ambiti quali il settore finanziario, l'industria 4.0, l'energia, i trasporti, la sanità e l'amministrazione elettronica sono essenziali per salvaguardare la sicurezza e la fiducia nelle attività e nelle operazioni online da parte dei cittadini, delle pubbliche amministrazioni e delle imprese» (considerando 39).

[11]Direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016.

[12]In particolare, ai sensi della direttiva NIS gli «operatori dei settori essenziali» sono coloro che svolgono la propria attività economica nel settore della fornitura e distribuzione dell'acqua potabile, dell'energia, dei trasporti, della salute, delle infrastrutture digitali, dei servizi bancari e finanziari; al contrario, sono definiti come «fornitori di servizi digitali» coloro che operano nel settore dei motori di ricerca, dei servizi di cloud computing e delle piattaforme di commercio elettronico. L'applicazione del citato principio di proporzionalità – *rectius*, gradualità – impone che gli obblighi di sicurezza previsti per i primi siano più severi rispetto a quelli previsti per i secondi, atteso il più alto livello di rischio per la stabilità nazionale in caso di attacchi informatici nei confronti degli OSE. In merito al campo di applicazione della direttiva, occorre segnalare le rilevanti modifiche formulate sul punto nella proposta di revisione del 16 dicembre 2020, COM(2020) 823 final (c.d. "direttiva NIS 2"), con la quale la Commissione europea ha manifestato l'intenzione di chiarire ed estendere la portata del precedente atto sia dal punto di vista soggettivo, ossia con riferimento

all'individuazione dei soggetti coinvolti nella catena di gestione del rischio cibernetico (introducendo al riguardo una nuova classificazione dei destinatari degli obblighi di sicurezza, che si divideranno in "essenziali" e "importanti"), sia dal punto di vista oggettivo, ossia con riferimento alla razionalizzazione degli obblighi di comunicazione e degli standard minimi di sicurezza.

[13]La necessità di promuovere una nuova strategia europea in materia di cybersicurezza viene ben rimarcata: nella comunicazione della Commissione e dell'Alto rappresentante dell'Unione del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 final, ove si riconosce, per la prima volta, che: «sempre più spesso gli attori statali raggiungono i loro obiettivi geopolitici non solo attraverso strumenti tradizionali come la forza militare, ma anche attraverso strumenti cibernetici più discreti, volti anche ad interferire nei processi democratici interni» (p. 2); nella comunicazione della Commissione del 19 febbraio 2020, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final, ove si precisa che: «Una vera trasformazione digitale deve iniziare dalla fiducia di cittadini e imprese europei nella sicurezza di prodotti e applicazioni. Quanto più siamo interconnessi, tanto più siamo vulnerabili alle attività informatiche dolose»; nella comunicazione della Commissione del 24 luglio 2020, *La strategia dell'UE per l'Unione della sicurezza*, COM(2020) 605 final, ove si sottolinea che: «L'avvento dell'Internet degli oggetti e il maggiore ricorso all'intelligenza artificiale comporteranno nuovi benefici ma anche una serie di nuovi rischi. [...] La dipendenza da sistemi online ha dato il via a un'ondata di attacchi da parte della cibercriminalità. Il cosiddetto "cybercrime as-a-service" (ossia l'offerta di servizi illegali) e l'economia "cibercriminale" sotterranea offrono un agevole accesso a prodotti e servizi informatici online offerti dalla criminalità informatica» (pp. 3-4); nella comunicazione della Commissione e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN(2020) 18 final, che aggiorna la precedente strategia del 2017.

[14]Si tratta di un fenomeno che ha acquisito un'importanza sempre crescente nell'agenda politica nazionale e dell'Unione a causa dell'accelerazione del processo di digitalizzazione riconducibile all'esperienza della pandemia da COVID-19 e del costante aumento degli episodi di attacchi cibernetici, legati da ultimo anche allo scoppio del drammatico conflitto tra Russia e Ucraina.

[15]In tal senso, si vedano le considerazione espresse nella Risoluzione del Parlamento europeo del 12 marzo 2019 sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione di quest'ultima per ridurre tali minacce, 2019/2575(RSP), ove si è chiarito come: «l'Unione debba assumere un ruolo guida in materia di cibersicurezza, adottando un approccio comune basato su un utilizzo efficiente ed efficace delle competenze dell'Unione, degli Stati membri e dell'industria, dato che un mosaico di decisioni nazionali divergenti nuocerebbe al mercato unico digitale [...]», e si «invita la Commissione a sviluppare una strategia che ponga l'Europa all'avanguardia nel settore delle tecnologie di cibersicurezza, onde ridurre la dipendenza dell'Europa dalla tecnologia straniera in tale campo».

[16]Regolamento UE 2019/881 del 17 aprile 2019 relativo all'Agenzia dell'Unione europea per la cybersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, che ha abrogato il precedente regolamento UE 526/2013 del 21 maggio 2013.

[17]Sul nuovo ruolo dell'Agenzia, cfr. A. Contaldo, D. Mula (a cura di), *Cybersecurity Law*, Pacini, 2020, p. 71 ss. In tema di cooperazione interistituzionale, occorre richiamare il regolamento UE 2021/887 del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza con l'obiettivo di colmare, nel contesto della rete dei Centri nazionali di coordinamento, il profondo divario di capacità e di competenze esistente nel territorio dell'Unione e di diffondere il più possibile i risultati delle ricerche e delle attività finanziate.

[18]Oltre che nei confronti del Dipartimento delle informazioni per la sicurezza (sul quale *infra*), il potere di direttiva del Presidente del Consiglio dei ministri è esercitato anche nei confronti dell'Agenzia informazioni e sicurezza esterna (AISE) e dell'Agenzia informazioni e sicurezza interna (AISI), le quali svolgono le rispettive attività di ricerca informativa sotto il coordinamento operativo del suddetto Dipartimento (art. 4, co. 3, lett. d-*bis*), l. 3 agosto 2007, n. 124).

[19]In particolare, ai sensi dell'art. 3, co. 1, lett. a) e b), d.P.C.M. 24 gennaio 2013, il Quadro strategico nazionale doveva contenere l'indicazione dei caratteri e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, interessati alla gestione dei sistemi e delle reti di interesse strategico, l'individuazione di strumenti e di procedure tramite i quali migliorare le capacità nazionali di prevenzione e risposta rispetto alle minacce del cyberspazio; il Piano nazionale per la protezione cibernetica doveva indicare, invece, gli obiettivi e le linee di azione da porre in essere per realizzare il predetto Quadro strategico.

[20]Art. 4, co. 1, d.P.C.M. 24 gennaio 2013. Il Comitato è presieduto dal Presidente del Consiglio ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico (art. 5, co. 3, l. 3 agosto 2007, n. 124).

[21]Cfr. art. 4, co. 3, lett. d-*bis*), l. n. 124/2007, introdotto dalla l. 7 agosto 2012, n. 133, e art. 7 d.P.C.M. 24 gennaio 2013 ai sensi del quale il DIS è chiamato, altresì, a trasmettere le informazioni e i dati rilevanti acquisiti al Nucleo per la sicurezza cibernetica, alle pubbliche amministrazioni e agli altri soggetti, pubblici e privati, interessati a ricevere tali informazioni.

[22]Artt. 8 e 9 d.P.C.M. 24 gennaio 2013.

[23]In particolare, il decreto ha rivisto le attribuzioni del Presidente del Consiglio dei ministri, del CISR e del Nucleo per la sicurezza cibernetica nelle situazioni di crisi informatica che coinvolgono aspetti di sicurezza nazionale, al fine di assicurare una risposta maggiormente unitaria e coordinata nella gestione e nella risoluzione delle predette ipotesi. Sulle novità introdotte dal d.P.C.M., si rinvia a L.V.M. Salamone, *La disciplina del* cyberspace *alla luce della direttiva europea delle reti e dell'informazione: contesto normativo nazionale di riferimento, ruolo dell'*intelligence *e prospettive* de iure condendo, in "federalismi.it", 2017, n. 23, p. 29 ss.

[24]Com'è noto, l'istituzione del Perimetro nazionale risponde all'esigenza di assicurare un livello elevato di sicurezza delle reti, dei sistemi e dei servizi informatici utilizzati da quei soggetti (pubbliche amministrazioni, enti pubblici e privati) che esercitano «una funzione essenziale dello Stato» o che prestano «un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato», seppur non rientranti nell'ambito di applicazione della citata direttiva NIS. Si tratta di soggetti individuati in un apposito elenco, adottato con d.P.C.M., su proposta del Comitato interministeriale per la cybersicurezza, non soggetto a pubblicazione o a istanze di accesso; sicché solo le amministrazioni e gli enti rientranti all'interno del suddetto Perimetro ricevono comunicazione dell'iscrizione (art. 1, co. 2-*bis*, d.l. 21 settembre 2019, n. 105).

[25]Accanto alla menzionata Agenzia, il d.l. n. 82/2021 ha istituito, presso la Presidenza del Consiglio dei ministri, il Comitato Interministeriale per la cybersicurezza (CIC), chiamato a svolgere funzioni consultive, di proposta e di vigilanza in materia di politiche di cybersicurezza del tutto assimilabili

a quelle in precedenza spettanti al CISR (il quale, nel nuovo assetto organizzativo, mantiene un ruolo importante nella gestione delle crisi cibernetiche, ai sensi degli artt. 4, co. 6, e 10 d.l. n. 82/2021).

[26]Le attività del CSIRT Italia sono definite dal d.P.C.M. dell'8 agosto 2019.

[27]In materia, va ricordato che la suddetta Agenzia: predispone la strategia nazionale di cybersicurezza (art. 7, co. 1, lett. b); è qualificata come «Autorità nazionale di certificazione della cybersicurezza» ai sensi dell'art. 58 del citato reg. UE 2019/881, con il compito di coordinare e di dirigere il sistema italiano di certificazione, qualificazione e valutazione della cybersicurezza dei prodotti, servizi e processi ICT (art. 7, co. 1, lett. e), come confermato, da ultimo, dal d.lgs. 3 agosto 2022, n. 123); è designata quale «Centro nazionale di coordinamento» ai sensi dell'art. 6 del citato reg. UE 2021/887, con il compito di supportare il Centro europeo di competenza per la cybersicurezza nell'attività di rafforzamento delle capacità, delle conoscenze e della competitività dell'Unione nel settore (art. 7, co. 1, lett. aa). Per un quadro riassuntivo delle funzioni della nuova Agenzia, si veda S. Aterno, *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, 2022, p. 234 ss.

[28]Sul punto, si vedano la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, cit., p. 6, ove si riconosce che: «Un approccio di "sicurezza fin dalla progettazione" adottato dai produttori di dispositivi connessi, software e attrezzature informatiche permetterebbe di definire la questione della cibersicurezza prima di immettere nuovi prodotti sul mercato. Questo potrebbe rientrare nel principio di "responsabilità", da elaborare ulteriormente insieme agli operatori del settore, che potrebbe ridurre le vulnerabilità dei prodotti/software applicando una serie di metodi che vanno dalla progettazione ai test e alla verifica, inclusa la verifica formale ove applicabile, la manutenzione a lungo termine e l'utilizzo di processi sicuri lungo il ciclo di sviluppo, così come lo sviluppo di aggiornamenti e correzioni atti a risolvere vulnerabilità precedentemente nascoste e rapidi interventi di aggiornamento e riparazione»; nonché la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, cit., par. 1.5., ove si precisa che il dovere di diligenza esigibile nei confronti dei produttori dovrà essere potenziato a livello normativo, proprio a causa della crescente diffusione del fenomeno dell'*Internet of things* di cui si è detto *supra*.

[29]Si tratta, invero, di un'obbligazione di non semplice esecuzione, dal momento che, come nota P.L. Montessoro, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in "Istituzioni del federalismo", 2019, n. 3, p. 790, oggi gli hacker investono ingenti risorse nella ricerca degli errori di programmazione (bug), al fine di modificare ad arte il comportamento del calcolatore in cui è inserito il programma difettoso. Sicché «il progettista deve correggere tutte le vulnerabilità del suo sistema, mentre all'hacker basta scoprirne una [...]».

[30]Sui possibili conflitti tra tutela della cybersicurezza e tutela della privacy, si è espresso in più occasioni lo stesso Garante europeo per la protezione dei dati, secondo il quale le recenti iniziative legislative in tema di *cybersecurity* non dovrebbero pregiudicare quanto già previsto dal GDPR, ma dovrebbero, al contrario, ispirarsi ai principi di quest'ultimo, come quelli del *privacy by design* e del *privacy by default* (art. 25 GDPR). Così, European Data Protection Supervisor, *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive*, 11 marzo 2021; nonché Id., *Opinion 8/2022 on the Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union*, 17 maggio 2022.

[31]Come affermato, da ultimo, da Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472; Id., sez. VI, 4 febbraio 2020, n. 881.

* * *

The cyber risk management in the algorithmic administrative decisions

Abstract: This contribution aims to highlight one of the main risks linked to the progress of the algorithmization of administrative decisions, that is the protection of cybersecurity. In particular, after having analyzed the complex multi-level system defined in recent years in the field of cybersecurity, the survey stresses the need to ensure an adequate level of cyber resilience in the automation of the various administrative procedures, drawing some systematic implications for the same legitimacy of the use of algorithmic formulas for decision-making process.

Keywords: Artificial intelligence – Algorithmic administrative decisions – Cybersecurity – Cyber risks