RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0241 • articolo sottoposto a peer review • pubblicato in anteprima il 28 ott. 2025

Francesco Midiri

Il ruolo delle autorità indipendenti nella regolazione del trattamento dei dati

Lo studio rileva che la normativa in materia di protezione dei dati personali, per il tramite della funzione di regolazione, viene attuata anche al di là del proprio ambito naturale di operatività fino a condizionare l'applicazione di altre discipline dell'ordinamento (quali quelle relative alla concorrenza, alla tutela dei lavoratori ed alla attività amministrativa algoritmica), in considerazione del fatto che essa viene percepita come la forma più adeguata di protezione dei diritti fondamentali nella civiltà digitale. Le autorità di regolazione, peraltro, debbono realizzare questa tendenza secondo un rigido principio di legalità, cioè attuando esclusivamente i compiti attribuiti dal GDPR: proteggere i dati personali garantendo, nel medesimo tempo, la libera circolazione delle informazioni per lo sviluppo economico sociale. Così, ad esempio, dovranno essere colpite le violazioni della *data protection* realmente lesive, cioè in grado di pregiudicare concretamente le libertà fondamentali. In caso contrario, le autorità genereranno una regolazione eccessivamente vincolistica introducendo, nei vari settori dell'ordinamento, regole e sanzioni che il legislatore non ha voluto.

Regolazione – Protezione dei dati personali – Garanzia dei diritti fondamentali – Principio di legalità

The role of independent regulatory authorities in the governance of data processing

The study highlights how *data protection* legislation, through regulatory functions, is being implemented beyond its natural scope, to the point of influencing the application of other legal provisions (such as those relating to competition, worker protection, and algorithmic administrative activity), given that it is perceived as the most appropriate form of protection of fundamental rights in the digital age. Regulatory authorities, however, must implement this trend according to a strict principle of legality, that is, by exclusively carrying out the tasks assigned by the GDPR: protecting personal data while simultaneously ensuring the free flow of information for economic and social development. Thus, for example, *data protection* violations that are truly harmful, i.e., those capable of concretely undermining fundamental freedoms, must be punished. Otherwise, the authorities will create overly restrictive regulation by introducing rules and sanctions in various areas of the legal system that the legislator did not intend.

Regulation – Protection of personal data – Guarantee of fundamental rights – Principle of legality

L'Autore è professore ordinario di Diritto amministrativo e pubblico nell'Università Cattolica del Sacro Cuore di Milano

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato* a cura di Marco Bombardelli, Simone Franca, Anna Simonati

Sommario: 1. L'applicazione della normativa di *data protection* fuori dal proprio ambito naturale di applicabilità ad opera della regolazione. – 2. I casi recenti di applicazione espansiva della *data protection* in differenti ambiti normativi – 3. Alcune considerazioni sull'ammissibilità di questa vocazione espansiva della normativa e della regolazione di *data protection*.

1. L'applicazione della normativa di *data protection* fuori dal proprio ambito naturale di applicabilità ad opera della regolazione

Per delineare il ruolo delle autorità amministrative indipendenti di *data protection* nella regolazione del trattamento dei dati non bisogna fare riferimento solo alle funzioni attribuite dalle disposizioni del GDPR (General Data protection Regulation, Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016)[1] le quali attribuiscono alle amministrazioni nazionali le competenze classiche di regolazione o di *command and control* (normative, di controllo, di vigilanza e di sanzione). Il tutto con i relativi problemi di "concentrazione" di funzioni di diversa natura in capo a medesimi soggetti pubblici e di "concentrazione" delle normative che le disciplinano[2].

Per cogliere, invece, la nuova *mission* complessiva che queste autorità stanno assumendo occorre considerare la loro tendenza attuale ad applicare la normativa di protezione dei dati personali anche oltre i suoi "naturali" ambiti di operatività. Ciò non significa che queste amministrazioni applichino regole di protezione dei dati personali al di fuori o in assenza del loro ordinario presupposto di applicazione, rappresentato dalla fattispecie di trattamento delle informazioni. Piuttosto, dopo che queste disposizioni sono state chiamate a regolare fenomeni di utilizzo delle informazioni, i Garanti le utilizzano per condizionare l'interpretazione e gli esiti applicativi di altre normative che regolano differenti materie del sistema giuridico, quasi come si trattasse di norme interposte. Il tutto come se le disposizioni di protezione nascessero nel trattamento dei dati ma andassero a morire in campi regolati da altre discipline, di cui condizionano il portato normativo.

Attraverso queste dinamiche la regolazione di *data protection* sta assumento un carattere espansivo, trasversale e totalizzante ed interessa progressivamente, unificandoli, vari settori normativi.

Certamente, questa tendenza è agevolata da alcuni caratteri fondamentali della normativa di protezione dei dati personali.

Innanzitutto, il diritto alla protezione dei dati personali si presenta come una situazione soggettiva formale e strumentale, cioè diretta ad ottenere l'applicazione dei principi e delle forme del GDPR come "strumento" per proteggere altri diritti fondamentali, consolidatisi nella tradizione giuridica europea[3]. Si tratta, quindi, di una pretesa divenuta ad ampio spettro, in grado di garantire posizioni attive diverse di segno culturale, sociale ed economico (dalla libertà di manifestare il proprio pensiero, al diritto all'assistenza sociale, alla possibilità di ottenere un mutuo). Per questo, la regolazione

1. Si tratta dei poteri conferiti dagli artt. 51, 57 e 58 del GDPR su cui sia consentito rinviare a Midiri 2019-a, Midiri 2019-b, Midiri 2019-c.
2. Problemi che la dottrina ha recentemente illustrato, cfr. Vettori 2024, con riferimento alle Autorità che regolano le dinamiche di mercato.
3. Sia consentito rinviare a Midiri 2017.

tende ad applicare questo diritto in maniera onnicomprensiva, in vari ambiti dell'agire umano.

Ancora, il principio di *accountability* (art. 5 GDPR)[4], ma ancora di più quelli di *privacy by default* e di *privacy by design* (art. 25 GDPR) rendono la normativa di protezione dei dati personali una disciplina non solo da attuare, ma, più propriamente, da tradurre in soluzioni pratico/operative determinate dalla *expertise* o dall'inventiva degli operatori. La regolazione delle autorità, infatti, realizza una naturale funzione di verifica di secondo livello della correttezza delle soluzioni organizzative e tecnologiche adottate dagli utilizzatori delle informazioni. Per questo, diventa una regolazione relativa al controllo delle scelte e delle soluzioni tecniche[5] e si espande, fisiologicamente, in ogni ambito delle attività realizzate con apparati tecnologici, meccanizzati o digitali (ad esempio, fino a regolare l'inclinazione ed il *focus* delle apparecchiature di videosorveglianza o la tipologia di informazioni registrate da apparecchi di geolocalizzazione che gestiscono la manutenzione di autoveicoli concessi in locazione).

Spinge nella direzione dell'estensione della regolazione di *data protection* anche la progressiva importanza assunta dalla base giuridica del legittimo interesse (GDPR art. 6, comma 1, lett. f) a discapito delle altre basi di derivazione civilistica – cioè radicate nel valore dell'equilibrio tra posizioni correlate in un rapporto diretto a realizzare contrapposti interessi – quali il consenso e la necessità di eseguire un contratto richiesto dall'interessato (GDPR art. 6, comma 1, lett. a e b)[6]. Infatti, considerata l'indeterminatezza della figura[7], che oscilla tra interessi non espressamente vietati ed interessi meritevoli di tutela per la loro funzionalità socio/economica, le autorità indipendenti si sentono in dovere di imporre fitte "reti di contenimento" normativo ai trattamenti fondati su questo presupposto di liceità[8]. Ed anche questo concorre a dilatare l'ambito di operatività della regolazione amministrativa.

Infine, l'impianto normativo del GDPR, pur con alcune differenziazioni, contempla un sistema disciplinare comune per il trattamento dei dati personali diretto a realizzare interessi privati e per quello diretto a realizzare, anche oggettivamente, interessi pubblici (come risulta dal combinato disposto degli artt. 6 e 55 del Regolamento)[9]. Anche così si rende espansiva la regolazione.

Considerate le ragioni dell'espansione dell'azione delle autorità amministrative di *data protection* è necessario considerare come essa si stia realizzando concretamente. A questo proposito, sembra che questa tendenza si produca in due modi diversi: attraverso un "recesso sostanziale" di altre discipline, che, per cosi dire, riducono il proprio ambito di applicazione in via interpretativa, in esito all'azione della giurisprudenza e della stessa regolazione; attraverso un "recesso formale" di altre discipline che riducono il proprio ambito di applicazione in via normativa, per effetto di specifiche disposizioni del legislatore.

Denominatore comune di queste due modalità, peraltro, è che l'espansione avviene, oltre che per i fattori già considerati, perché la *data protection* viene sostanzialmente percepita come uno strumento più adeguato ed efficace per garantire i diritti fondamentali. In altri termini, è un criterio interpretativo e normativo di prevalenza a dettare l'espansione della regolazione.

2. I casi recenti di applicazione espansiva della *data protection* in differenti ambiti normativi

È possibile tracciare una panoramica di esempi delle forme di recesso di cui sopra.

4. Sul quale Galli 2023.
5. Su questi temi Yeung–Bygrave 2022, spec. p. 141.
6. Cfr. su questa base giuridica le recenti indicazioni generali di European Data Protection Board, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, Versione 1.0, 8 ottobre 2024.
7. Recentemente, Bonomi Madec–Vasileiadou 2025.
8. Sottolinea come questa azione regolatoria si traduca in una sistematica imposizione dell'interesse pubblico alla correttezza di trattamento Proietti 2022.
9. Il tema del trattamento pubblico dei dati è stato recentemente illustrato da Franca 2023.

Con la nota sentenza C-252 del 2023 (*Meta Platform*) la Corte di giustizia Ue[10] dà corso al recesso della normativa a tutela della concorrenza a vantaggio di quella di *data protection*. I Giudici, nel valutare l'irrogazione di una sanzione antitrust dell'autorità tedesca, affermano che l'"incrocio" di dati personali (cioè la trasmissione delle preferenze dei clienti ad investitori pubblicitari) da parte di un social network è illecito con riguardo alla disciplina del loro trattamento. Infatti, esso non trova fondamento giuridico né nel consenso dell'interessato, né nella necessità di eseguire il contratto di utilizzo della rete sociale, né in un legittimo interesse del titolare.

L'elemento rilevante della sentenza, però, è che la violazione delle regole del GDPR rappresenta l'elemento costitutivo della fattispecie di abuso di posizione dominante di cui all'art. 102 del TFUE. In altri termini, un trattamento illecito di dati personali può rappresentare lo strumento per alterare le dinamiche della concorrenza. Per questo, secondo la Corte, le autorità antitrust nazionali, prima di irrogare una sanzione per un comportamento anticoncorrenziale, determinato da una pretesa violazione del diritto alla protezione dei dati personali, debbono fare riferimento ai precedenti provvedimenti sanzionatori delle autorità di *data protection*, per considerare se il comportamento di cui è causa sia stato precedentemente qualificato come illecito. Conseguentemente debbono attenersi alla "giurisprudenza" o prassi regolatoria delle autorità. Nel caso, poi, in cui non vi siano precedenti regolatori in termini, la sentenza impone alle autorità antitrust di coinvolgere nel procedimento i Garanti per la protezione dei dati personali, fornendo loro un termine entro il quale qualificare i comportamenti in esame. Solo spirato questo termine, le amministrazioni procedenti antitrust potranno assumere le loro determinazioni sanzionatorie[11].

Come si vede, la Corte impone un recesso della regolazione (e della normativa) antitrust a vantaggio di quella di *data protection*, chiamata ad identificare i trattamenti scorretti di informazioni personali sostanzialmente in grado di alterare illecitamente anche le dinamiche di mercato. È interessante considerare, poi, come, in questo caso di recesso, la normativa sul trattamento dei dati personali vada oltre la propria *mission* originaria di protezione dei diritti fondamentali, per ridondare nella garanzia degli interessi del mercato.

Un altro interessante esempio di recesso formale è rappresentato dalla sentenza del Consiglio di Stato n. 497 del 2024 che ripropone lo stesso itinerario argomentativo della Corte di giustizia, collocandolo, però, nella materia della tutela del consumatore. In questo caso, i giudici valutano l'applicazione di sanzioni irrogate dall'autorità antitrust a tutela dei consumatori ed affermano che una società commerciale che fornisce ai propri clienti informazioni ingannevoli sull'utilizzo dei loro dati personali (trasmessi senza consenso ad inserzionisti commerciali che li utilizzano per concludere nuovi contratti) li utilizza in maniera scorretta ai sensi del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, art. 130). Ma questo comportamento rappresenta anche l'elemento costitutivo della violazione dei diritti dei consumatori attribuiti dall'art. 67-*sexdecies* del Codice del consumo (d.lgs. 6 settembre 2005, n. 206) che li protegge dalle comunicazioni commerciali non richieste[12].

10. Corte giustizia Ue, Grande Sezione, sent. 4 luglio 2023, n. 252, in "Foro it."2023, 12, IV, 580.

11. Sulle dinamiche di coordinamento delle autorità cfr. per tutti Manzini 2023; Parona 2024.

12. La sentenza segue nella sostanza la precedente giurisprudenza dello stesso Consiglio di Stato (Consiglio di Stato, Sez. VI, 29 marzo 2021, n. 2630, in "Dejure" e Consiglio di Stato, Sez. VI, 29 marzo 2021, n. 2631 in "Foro it.", 2021, 6, III, 325) che aveva affermato, con una ricostruzione normativa differente, perché non ancora condizionata dalla giurisprudenza della Corte di giustizia Ue, che una violazione degli obblighi di informazione del GDPR avrebbe potuto rilevare non in sé stessa, ma come violazione degli obblighi a tutela dei consumatori, che avrebbe rappresentato l'unico illecito giuridicamente rilevante. Le sentenze avevano la singolare intenzione di limitare l'applicazione diretta della *data protection* in ambito economico evitando che il GDPR erodesse l'applicazione delle altre discipline astrattamente applicabili ed estendesse "il proprio ambito di applicazione fin dove può giungere qualsiasi forma di relazione umana o automatica del dato personale", p. 23 sent. 2631. Per questo, i giudici avevano limitato la *data protection* affermando che essa protegge solo i diritti personalissimi e non quelli di segno economico, rimessi alla tutela di altre normative. Il tentativo, peraltro, non aveva condotto a

I giudici, correlativamente, affermano il necessario coinvolgimento, nella procedura di irrogazione di sanzioni a tutela del consumatore, del Garante per la protezione dei dati personali, proprio perché l'illecito consumeristico è realizzato violando la normativa di *data protection*, le cui modalità di applicazione non possono che essere determinate dalla relativa amministrazione di regolazione.

Anche in questo caso, come nella giurisprudenza della Corte di giustizia, la normativa e la regolazione di tutela del consumatore recedono a vantaggio della normativa e della regolazione a tutela dei dati personali. Qui, però, siamo di fronte a discipline e funzioni amministrative che hanno tutte lo stesso obiettivo di proteggere i diritti fondamentali di segno economico delle persone. La protezione dei dati personali, però, viene fatta prevalere, perché è percepita come più efficace. Infatti, i giudici le lasciano l'ultima parola sulle modalità di garanzia delle ragioni del consumatore.

Un altro esempio di recesso sostanziale è rappresentato dalla giurisprudenza italiana recente in materia di controlli difensivi in senso stretto (ovvero quei controlli realizzati *ex post* dal datore di lavoro nei confronti di lavoratori con riguardo ai quali sia sorto il sospetto che abbiano violato i propri doveri o abbiano pregiudicato gli interessi dell'azienda) ed in particolare dalla sentenza della Corte di Appello di Venezia di data 22 maggio 2024[13].

Questi controlli sono tradizionalmente sottratti dalla giurisprudenza dall'ambito di applicazione dell'art. 4 dello Statuto dei lavoratori (legge 40 maggio 1970, n. 300), che li sottopone al rispetto dei principi del Codice in materia di protezione dei dati personali. Nonostante ciò, la sentenza afferma che questo tipo di verifiche, nella fattispecie indagini e investigazioni private, debbono sottostare alla *data protection*. Questo perché, sulla scorta degli insegnamenti della giurisprudenza CEDU[14], incidono sulla dignità del lavoratore e, per essere sostenibili, con riferimento ai diritti fondamentali, debbono osservare i principi di necessità, proporzionalità, legittimità delle finalità, ecc… della normativa che protegge i dati personali. E questi principi sono attuati, qui, dalla regolazione del Garante nazionale[15]. Sulla base di queste considerazioni, quindi, i giudici nazionali affermano che le investigazioni difensive dirette a verificare l'autenticità dello stato di malattia, ulteriori rispetto agli accertamenti delle autorità pubbliche, sono incongrue se contrarie alle linee guida in materia poste dall'Autorità di protezione dei dati personali. E questo rende illecito il conseguente licenziamento.

Anche in questo caso, nella sostanza, l'illecito di *data protection* integra l'elemento costitutivo di un illecito lavoristico ed è possibile ipotizzare che, nel prossimo futuro, la giurisprudenza italiana, proprio come hanno fatto i giudici europei, affermi in maniera esplicita e formale questa dinamica.

Occorre considerare che, in questo caso, la protezione dei dati ed il diritto del lavoro condividono l'obiettivo di proteggere i diritti fondamentali. Tuttavia, il prevalere della prima normativa – che impone determinate modalità di trattamento dei dati, considerate maggiormente "sostenibili" con riferimento alla protezione della dignità personale – supera la logica lavoristica, modellata sulla ricerca dell'equilibrio di posizioni corrispettive

limitare nel concreto la normativa di protezione dei dati personali che era riuscita a condizionare nella sostanza se non nella forma i canoni di applicazione della disciplina di tutela del consumatore. Sulle sentenze Franca 2021; sia consentito rinviare anche a Midiri 2021.

13. In "Il lavoro nella giurisprudenza", 2024, p. 1135 con nota di M. D'Aponte 2024 che cita come precedenti in termini Cass. n. 17723/2017; Cass. n. 25732/2021; Cass. n. 18168/2023.

14. SI fa riferimento alla nota sentenza della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 – Ricorso n. 61496/08 – *Barbulescu c. Romania*.

15. A questo proposito la sentenza cita le "Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria" (Provvedimento del Garante per la protezione dei dati personali n. 60/2008) poi trasposte nelle Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 – 19 dicembre 2018 (Pubblicato sulla Gazzetta Ufficiale n. 12 del 15 gennaio 2019) Registro dei provvedimenti n. 512 del 19 dicembre 2018.

collegate in un rapporto bilaterale datore di lavoro/lavoratore. In altri termini, si impongono modalità di svolgimento di attività private (oggetto di regolazione amministrativa pubblica) piuttosto che regole di equilibrio di una relazione giuridica.

Nella dimensione del diritto del lavoro, peraltro, è possibile rilevare anche dinamiche di recesso "formale" oltre che sostanziale. Infatti, lo stesso art. 4 dello Statuto dei lavoratori, che, come abbiamo visto, fa riferimento ai controlli difensivi in senso ampio (cioè quei controlli sistematici per la difesa soprattutto dei beni aziendali) impone, nella loro realizzazione, l'applicazione dei principi di protezione dei dati personali. In questo caso, è lo stesso legislatore a disporre che la normativa di protezione dei dati personali condizioni gli esiti applicativi del diritto del lavoro e del diritto sindacale. Correlativamente, il Garante ha sviluppato un'intensa attività di regolazione che disciplina lo svolgimento di attività come la videosorveglianza, il controllo della posta elettronica aziendale, l'analisi dei metadati dei computer aziendali[16]. In sostanza, l'amministrazione pone le coordinate normative all'interno delle quali, ferma l'applicazione delle regole di diritto del lavoro e delle dinamiche sindacali, debbono svolgersi i poteri di controllo, disciplinari e sanzionatori del datore di lavoro. Anche in questo modo, le violazioni della *data protection* finiscono per rappresentare, sostanzialmente, l'elemento costitutivo di illeciti giuslavoristici.

Esistono, ancora, casi di recesso sostanziale in grado di produrre i propri effetti nella dimensione dell'attività amministrativa e del provvedimento.

La Corte di giustizia Ue ha pronunciato alcune recenti sentenze nelle quali si è interrogata sulla legittimità giuridica generale di decisioni di *credit scoring* (cioè della attribuzione interamente automatizzata a un cliente di un servizio finanziario di un punteggio che determina la sua solvibilità e, quindi, il possibile accesso a rapporti contrattuali di varia natura). Con la sentenza C-634/2023 (*Schufa*)[17] la Corte risolve il problema utilizzando un parametro normativo tratto dalla *data protection*, ovvero l'art. 22 del GDPR (rubricato "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione").

I Giudici, a questo riguardo, affermano che il *credit scoring* è qualificabile come una decisione interamente automatizzata, perché incide sulla sfera giuridico-soggettiva del destinatario. Nello stesso tempo affermano che essa è lecita, in senso generale, se fondata sui presupposti di legittimità di trattamento dello stesso art. 22: la presenza di una norma di diritto europeo o nazionale – anche di una disposizione che disciplini attività di interesse pubblico – che l'autorizzi, garantendo il rispetto dei diritti fondamentali; la messa a disposizione di procedure di reclamo con intervento umano che assicurino la correttezza di merito della decisione; il rispetto di tutti i principi normativi generali della protezione dei dati personali (ovvero tutti quelli indicati negli artt. 5, 6 e 25 del GDPR).

Viene affermato con decisione, quindi, che un atto interamente automatizzato, anche adottato in assenza di un intervento umano, è pienamente lecito se è previsto dalla legge, ma, soprattutto, se segue tutti i parametri di trattamento delle informazioni personali, parametri che ne rappresentano il vero metro di ammissibilità.

La sentenza supera la *vulgata* pubblicistica, consolidatasi recentemente, secondo la quale un provvedimento amministrativo privo dell'intervento umano nella sua fase di formazione sarebbe illegittimo[18], a più forte ragione se di carattere discrezionale[19]. Impone, invece, come nuovi parametri di liceità, prima che di legittimità, i principi della *data protection*.

In questa nuova ricostruzione, allora, principi come la funzionalizzazione del trattamento dei dati (alla base della decisione automatizzata) per le finalità legittime previste dalla legge, la correttezza del trattamento stesso e la veridicità dei dati finiranno per rappresentare, nella dimensione provvedimentale, una versione aggiornata di categorie

16. Fragassi 2024. Ma in generale su tutti i temi relativi ai controlli difensivi cfr. la panoramica di Rotondi–Tursi 2025.
17. Corte giustizia Ue, sez. I, 7 dicembre 2023, causa C-634/21, in "Nuova giurisprudenza civile commentata", 2024, 416, con nota di D'Orazio 2024, sulla sentenza anche Pietrella–Racioppi 2024.
18. Per tutti Stacca 2024; Grenci 2024.
19. In questi casi, come afferma la giurisprudenza, la discrezionalità verrebbe riallocata "a monte" nella definizione dell'algoritmo, su questi temi Botto 2024 e bibliografia ivi citata.

come l'eccesso di potere per sviamento, la contraddittorietà tra atti del procedimento, l'incompletezza dell'istruttoria o il travisamento dei fatti. Certamente, si tratta di nuovi parametri che non sostituiranno i vecchi, primo fra tutti il canone della trasparenza, su cui tanto ha insistito a ragione la dottrina[20], ma si affiancheranno ad essi, per fondare un nuovo sindacato di legittimità del provvedimento algoritmico. Ed è inutile dire che tutti questi parametri, in futuro, saranno definiti, nel concreto, dalla regolazione amministrativa.

Tutti questi parametri saranno utili per contestare decisioni algoritmiche sbagliate, anche senza passare dalla piena conoscenza dei modelli che hanno guidato i sistemi (modelli che nella IA sono irrecuperabili agli stessi programmatori per i noti fenomeni di *black box*). Proprio come ha sostanzialmente fatto una recente sentenza della Corte di giustizia che ha ipotizzato l'irragionevolezza di una decisione di *credit scoring* che non ammetteva una persona ad un contratto telefonico con canone di soli dieci euro al mese per i suoi trascorsi di cattivo pagatore[21]. Ma in quest'ottica appariranno implausibili anche gli algoritmi di assegnazione degli incarichi di insegnamento ai supplenti precari che attribuiscono incarichi didattici a persone con punteggio inferiore e li negano ad altre con punteggio superiore, violando il principio di verità dei dati personali prima di quello di efficacia della funzione di istruzione[22].

Per concludere sul punto, anche nel caso del *credit scoring*, la normativa di protezione dei dati personali si impone come parametro di liceità giuridica generale per la sua maggiore capacità di proteggere i diritti della persona con riguardo allo svolgimento di ogni attività automatizzata, pubblica o privata, ammessa dalla legge.

Sono stati indicati i casi più recenti e rilevanti di recesso sostanziale e formale, ma occorre considerare che non si tratta degli unici. In vari altri campi, infatti, è la stessa regolazione ad imporre, all'interno di sistemi normativi specifici, norme *ad hoc*, che rappresentano lo sviluppo o l'adattamento di regole generali di *data protection*. Ad esempio, l'EDPB ha recentemente imposto alcune prescrizioni specifiche per l'utilizzo di modelli di intelligenza artificiale[23], indipendentemente dall'applicazione del recente regolamento europeo in materia[24]. Ancora, il Garante italiano ha emanato un vademecum sulla privacy a scuola che introduce regole in grado di incidere sulle modalità di svolgimento dell'attività didattica (come la definizione di tracce di temi o la loro lettura in classe, le modalità di svolgimento della videolezione, il controllo dei docenti sull'utilizzo di social network per prevenire fenomeni di cyberbullismo o simili)[25].

3. Alcune considerazioni sull'ammissibilità di questa vocazione espansiva della normativa e della regolazione di *data protection*

Esaurita questa panoramica è possibile considerare come, per il tramite della regolazione, si stia realizzando un'estensione sostanziale dell'ambito di

20. Carloni 2024.
21. Corte giustizia Ue, sez. I, sent. 27 febbraio 2025, causa C-203/22, pur anche in questo caso affermando l'obbligo di trasparenza anche in presenza di segreti industriali.
22. Cfr. Tribunale di Roma, sent. n. 1463/2023 pubbl. il 10 febbraio 2023 sulla quale Rivellini 2023, ma ancora più chiara, tra le altre di medesimo tenore, Tribunale di Torino, sent. n. 1232/2025 del 15 maggio 2025. In estrema sintesi, l'algoritmo ministeriale consentiva ai docenti, prima dell'inizio dell'anno scolastico, di identificare una serie di scuole di loro preferenza. Una volta effettuato il primo giro di chiamate senza che si fossero rese disponibili scuole di loro gradimento il sistema considerava questi stessi docenti rinunciatari su tutte le scuole (anche quelle scelte) per tutte le eventuali tornate successive (forse per ragioni legate ad una più agevole programmazione degli algoritmi). Resisi disponibili successivamente incarichi nelle scuole di preferenza i docenti venivano logicamente pretermessi ed il sistema procedeva alla chiamata di altri docenti, naturalmente collocati più in fondo nelle liste e con minore punteggio.
23. Cfr. European Data Protection Board, *Opinion n. 8/2024 on certain data protection aspects related to the processing of personal data in the context of AI models* (adottata il 17 dicembre 2024).
24. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024.
25. Cfr. Garante per la protezione dei dati personali *Vademecum La scuola a prova di privacy*, 2023.

applicazione della disciplina della *data protection*. Essa tende oggi ad identificarsi con l'ambito della protezione dei diritti fondamentali e, più, in generale, della dignità della persona nei confronti delle attività umane realizzate con strumenti tecnologici, cioè di tutte[26]. In sostanza, si scrive protezione dei dati personali ma si legge garanzia dei diritti inviolabili dell'uomo, secondo il riferimento classico del nostro art. 2 della Costituzione. Si tratta di una tendenza ormai irreversibile di politica del diritto a cui è necessario adattarsi.

Peraltro, da un punto di vista giuridico, non è necessario fare considerazioni di ordine politico o sociale e chiedersi se si tratta di una tendenza efficace o utile. È necessario, invece, chiedersi se si tratti di una tendenza ammissibile nell'ambito delle coordinate giuridico istituzionali europee e nazionali. Non si deve dimenticare, infatti, che spesso queste forme di recesso conducono all'applicazione di norme derivate dalla protezione dei dati personali in ambiti nei quali il legislatore non le ha volute o all'irrogazione di conseguenti sanzioni per infrazioni non direttamente previste in differenti settori disciplinari.

La soluzione sembra potere essere quella, classica ma sempre attuale[27], di applicare un rigido principio di legalità riferito alle norme attributive ed alle condizioni di validità del potere di regolazione, che è il vero strumento di questa estensione sostanziale. Non si tratta, come si vede, di utilizzare il principio di legalità come parametro di legittimità per le attività di trattamento pubbliche e private, come ha ben fatto la dottrina recente[28], ma di applicarlo per condizionare le differenti funzioni delle amministrazioni di regolazione, che controllano, sanzionano e disciplinano quelle attività.

Applicare il principio di legalità alle funzioni di regolazione delle amministrazioni indipendenti nazionali ed europee significa imporre, come obiettivi e come coordinate fondamentali delle loro competenze, i due interessi pubblici che il legislatore europeo ha posto a fondamento del GDPR: la tutela dei diritti fondamentali e la libera circolazione dei dati personali (art. 1 ed art. 55 per le Autorità). I Garanti del trattamento dei dati debbono esercitare le loro funzioni tenendo conto che si tratta dei due pilastri fondamentali della *data protection* e che, nell'attuazione della normativa (vera *mission* delle Autorità ex art. 55 del GDPR), debbono essere realizzati insieme e debbono rimanere integrati e coordinati. In caso contrario, si scivolerà verso una disciplina squilibrata, esclusivamente difensiva, formalistica ed in grado di condizionare oltremisura anche tutti i campi di attività dove la protezione dei dati personali viene "esportata".

Tutto ciò può essere realizzato esercitando le funzioni di regolazione secondo un rigido principio di "lesività" delle attività di trattamento. In altri termini, le amministrazioni indipendenti, nella loro normazione di carattere tecnico, nella qualificazione degli illeciti e nell'applicazione delle sanzioni, dovranno identificare, come comportamenti sostanzialmente contrari alle regole dell'ordinamento, quelli in grado, non soltanto di violare forme, procedure, obblighi o principi del GDPR, ma quelli in grado di recare pregiudizio reale ai diritti inviolabili garantiti attraverso il diritto alla protezione dei dati personali. In caso contrario, la protezione dei dati perderà il suo equilibrio, ma anche la sua ragione d'essere, che è quella di rendere lo sviluppo tecnologico sostenibile e compatibile con la dignità umana.

Del resto, la stessa giurisprudenza in materia di risarcimento del danno da trattamento illecito dei dati, pur relativa ad altra materia, afferma il principio secondo il quale una violazione delle disposizioni del GDPR non è di per sé sufficiente a costituire un "danno risarcibile"[29].

26. Cfr. a questo proposito Simoncini 2023, che afferma che la tecnologia è ormai trasversale e necessaria per ogni aspetto della vita umana. È utile e veloce ma con un incomparabile impatto sui diritti. Diventa un potere privato che serve ad informare ed a sostituire la decisione umana, ovvero un potere nei confronti del quale si registra la inadeguatezza della normazione parlamentare classica a vantaggio della self regulation e coregulation.
27. Si tratta di un principio che giovani studiosi hanno utilmente utilizzato per risolvere questioni anche più complesse cfr. per tutti Vaccari 2024; Vettori 2024.
28. Ponti 2023.
29. Corte giustizia Ue, sez. VIII, 4 ottobre 2024, causa C-507/23; Corte giustizia Ue, sez. III, 20 giugno 2024, causa C-590/22; Corte giustizia Ue, sez. III, 11 aprile 2024, causa C-741/21.

Riferimenti bibliografici

S. Bonomi Madec, G. Vasileiadou (2025), *Understanding Legitimate Interest under the GDPR: A study of the CJEU Case C-621/22 and the EDPB Guidelines*, in "Global Privacy Law Review", vol. 6, 2025

G. Botto (2024), *Decisone algoritmica, discrezionalità e sindacato del giudice amministrativo*, in "Federalismi.it", vol. 17, 2024

E. Carloni (2024), *Transparency within the artificial administration, principles, paths, perspectives and problems*, in "Italian Journal of Public Law", vol. 16, 2024

M. D'Aponte (2024), *I controlli difensivi devono soggiacere ai principi di giustificatezza, proporzionalità e minimizzazione dei dati trattati*, in "Il Lavoro nella Giurisprudenza", vol. 12, 2024

F. D'Orazio (2024), *Il credit scoring e l'art. 22 del GDPR al vaglio della Corte di giustizia*, in "Nuova Giurisprudenza Civile Commentata", vol. 2, 2024

A. Fragassi (2024), *L'instabile equilibrio tra controllori e controllati nello sguardo del Garante privacy*, in "Labour & Law Issues", vol. 10, 2024

S. Franca (2023), *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Editoriale Scientifica, 2023

S. Franca (2021), *L'intreccio fra disciplina delle pratiche commerciali scorrette e normativa in tema di protezione dei dati personali: il caso Facebook approda al Consiglio di Stato*, in "Rivista della Regolazione dei Mercati", vol. 2, 2021

F. Galli (2023), *Il principio di accountability*, in L. Califano, V. Fiorillo, F. Galli (a cura di), "La protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale", Giappichelli, 2023

S.B. Grenci (2024), *Le applicazioni di Intelligenza artificiale a supporto dell'automazione del procedimento amministrativo*, in "Rivista Italiana di Informatica e Diritto", 2024, n. 1

P. Manzini (2023), *Antitrust e privacy: la strana coppia*, in Id. (a cura di), "I confini dell'antitrust – Diseguaglianze sociali, diritti individuali, concorrenza", Giappichelli, 2023

F. Midiri (2021), *Proteggere i dati personali con le tutele del consumatore*, in "Giornale di Diritto Amministrativo", vol. 5, 2021

F. Midiri (2019-a), *Commento all'art. 51, Regolamento UE 27 aprile 2016, n. 2016/679 in materia di protezione dei dati personali (c.d. GDPR)*, in A. Barba, S. Pagliantini (a cura di), "Commentario del Codice Civile", Utet, 2019

F. Midiri (2019-b), *Commento all'art. 57, Regolamento UE 27 aprile 2016, n. 2016/679 in materia di protezione dei dati personali (c.d. GDPR)*, in A. Barba, S. Pagliantini (a cura di), "Commentario del Codice Civile", Utet, 2019

F. Midiri (2019-c), *Commento all'art. 58, Regolamento UE 27 aprile 2016, n. 2016/679 in materia di protezione dei dati personali (c.d. GDPR)*, in A. Barba, S. Pagliantini (a cura di), "Commentario del Codice Civile", Utet, 2019

F. Midiri (2017), *Il diritto alla protezione dei dati personali*, Editoriale Scientifica, 2017

L. Parona (2024), *Addressing the interplay between competition law and data protection law in the digital economy through administrative cooperation: the CJEU judgment in the Meta Platforms case*, in "Italian Journal of Public Law", vol. 16, 2024

V. Pietrella, S. Racioppi (2024), *Il credit scoring e la protezione dei dati personali: commento alle sentenze della Corte di giustizia dell'Unione europea del 7 dicembre 2023*, in "Rivista Italiana di Informatica e Diritto", 2024, n. 1

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

G. Proietti (2022), *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in "Contratto e Impresa", vol. 3, 2022

G. Rivellini (2023), *L'errore dell'algoritmo obbliga la pubblica amministrazione a risarcire il danno*, in "www.irpa.eu – Osservatorio sullo Stato digitale", 14 giugno 2023

F. Rotondi, A. Tursi (2025), *I controlli sull'attività dei lavoratori alla prova dell'intelligenza artificiale*, in "Il Lavoro nella giurisprudenza", vol. 2, 2025

A. Simoncini (2023), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di Stato e forma di governo*, in Id. (a cura di), "Sistema delle fonti e nuove tecnologie. Il ruolo delle autorità indipendenti", Giappichelli, 2023

S. Stacca (2024), *Potere algoritmico. Profili organizzativi del rapporto tra amministrazione e automazione*, in "Diritto Pubblico", vol. 2, 2024

S. Vaccari (2024), *L'invalidità parziale del provvedimento amministrativo*, Giappichelli, 2024

N. Vettori (2024), *Autorità indipendenti e concentrazione dei poteri: distinzione delle funzioni a garanzia dei diritti*, Editoriale Scientifica, 2024

K. Yeung, L.A. Bygrave (2022), *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*, in "Regulation & Governance", vol. 16, 2022