Raffaella Dagostino
Professore Associato di Diritto Amministrativo, presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Foggia
raffaella.dagostino@unifg.it

La gestione dei dati nell'era digitale: un difficile bilanciamento fra esigenze di sicurezza, trasparenza e solidarietà

Data governance in the digital eRa: a difficult balance between security, transparency and solidarity needs

Sintesi

Il tema del trattamento dei dati in possesso della p.a. sta acquisendo sempre maggiore importanza per via dello sviluppo digitale che ha notevolmente incrementato la capacità di raccolta, catalogazione e circolazione dei dati, sia da parte della p.a. sia dei soggetti privati (c.d. gatekeeper ossia i gestori delle piattaforme digitali).

Ne è ben consapevole il legislatore europeo che ha di recente messo a punto una "strategia europea per i dati", adottando il Reg. UE 2022/1925 sui mercati digitali (c.d. D.M.A.), volto a regolamentare i rapporti fra imprese che forniscono servizi di piattaforma e imprese che erogano servizi digitali; il Reg. UE 2022/2065 in materia di mercato unico dei servizi digitali (c.d. D.S.A.), proteso a garantire la creazione di un ambiente on line sicuro; nonché il Reg. UE 2022/868 sulla Governance europea dei dati.

L'implementazione della disciplina europea dimostra che il problema della protezione dei dati non può più essere confinato a un approccio di tipo "tradizionale", fatto proprio dallo stesso GDPR, ossia incentrato sulla tutela del diritto alla privacy (intesa come autodeterminazione informativa), espressione del diritto del singolo individuo, titolare del dato, a veder tutelata la propria riservatezza o l'integrità del dato nei confronti del titolare del trattamento.

È, infatti, cresciuta in maniera esponenziale la rilevanza e la dimensione collettiva della protezione dei dati per via dell'implementazione di meccanismi di raccolta di massa di una pluralità di dati dei cittadini (è il caso dei c.d. big data analytics incentivati dall'uso delle tecnologie e degli strumenti d'intelligenza artificiale: si pensi all'uso dei dispositivi IoT – Internet of things of machines), anche da parte dei pubblici poteri (ad esempio, si pensi alla raccolta dati per ragioni di sorveglianza e controllo democratico, a alla raccolta di dati biometrici), nonché l'esigenza di garantire una maggiore interoperabilità dei dati fra settore pubblico e privato, non solo per ragioni economiche dettate dal mercato digitale, bensì per finalità altruistiche, a beneficio della società (si può pensare, ad esempio, all'importanza della condivisione delle informazioni sulla salute del paziente fra operatori sanitari pubblici e privati).

Ciò imporrebbe, a carico della p.a., l'adozione di un approccio di tipo proattivo, in primis, nel rafforzamento della governance dei dati e nella gestione dei rischi correlati, nonché uno sforzo ulteriore proteso a garantire il superamento del *digital divide* esistente in Italia che, di fatto, compromette l'effettività dell'azione amministrativa e l'erogazione di servizi pubblici essenziali nei contesti in cui il rapporto giuridico amministrativo risulti dematerializzato.

Pertanto, s'intravedono nuovi scenari d'intervento pubblico ai fini del trattamento e della circolazione dei dati, con conseguente possibile implementazione dell'apparato amministrativo e rafforzamento dell'esercizio di funzioni non solo di regolazione, controllo e sanzione, bensì verosimilmente, anche di amministrazione attiva, a garanzia di un difficile equilibrio fra sicurezza, trasparenza e solidarietà.

ABSTRACT

The issue of data processing in the possession of the public administration is becoming increasingly important due to digital development, which has significantly increased the ability to collect, catalog and circulate data, both by the public administration and by private entities. So, the European legislator

has recently developed a "European strategy for data", adopting EU Reg. 2022/1925 on digital markets (so-called D.M.A.), aimed at regulating the relationships between companies that provide platform services and companies that provide digital services; EU Reg. 2022/2065 on the single market for digital services (so-called D.S.A.), aimed at ensuring the creation of a secure online environment; as well as EU Reg. 2022/868 on European Data Governance. The implementation of the European framework demonstrates that there is a need for a strengthening data governance and the management of related risks, as well as a further effort to ensure that the digital divide existing in Italy is overcome, which, in fact, compromises the effectiveness of administrative action and the provision of essential public services in contexts where the administrative legal relationship is dematerialized. Therefore, new scenarios of public intervention for the purposes of data processing and circulation are foreseen, with the consequent possible implementation of the administrative apparatus and strengthening of the exercise of administrative functions such as regulation, control and sanction, to guarantee a difficult balance between security, transparency and solidarity.

PAROLE CHIAVE: Gestione dei dati – Ordinamento digitale – Trasparenza – Solidarietà – Funzioni amministrative

KEYWORDS: Data governance – Digital order – Transparency – Solidarity – Administrative functions

1. La governance dei dati nell'era digitale

Il tema della gestione dei dati sta acquisendo sempre maggiore importanza nella società odierna, per via dello sviluppo digitale che ha notevolmente incrementato la capacità di raccolta, catalogazione e circolazione dei dati medesimi, sia da parte della pubblica amministrazione sia dei soggetti privati (c.d. *gatekeeper*, ossia i gestori delle piattaforme digitali).

Come noto, la tecnologia e il ricorso a strumenti di intelligenza artificiale, nel corso di questi ultimi anni[1], hanno notevolmente inciso sulle modalità di esercizio di attività economiche, sulle modalità di erogazione di alcuni servizi pubblici essenziali (sanità, istruzione, trasporti), sulle forme di partecipazione democratica alla vita sociale e finanche sui comportamenti dei singoli individui, comportando un inesorabile processo di trasformazione economica, sociale e culturale della società contemporanea.

In un contesto sempre più deterritorializzato e dematerializzato, espressione di una società fluida, liquida[2], i dati, più o meno consapevolmente immessi in rete, generati e rilasciati dai singoli individui, costituiscono un elemento centrale di questa trasformazione, tanto da essere indicati come "il nuovo petrolio" della società moderna[3], sempre più protesa verso l'implementazione della c.d. *data economy*.

Tale espressione, come noto, sta ad indicare l'esistenza di una economia reale dei dati, basata sulla capacità, delle istituzioni e delle imprese, di gestire una quantità sempre crescente di informazioni digitali. Quindi, un'economia in cui istituzioni e imprese sono chiamate a interpretare correttamente i dati con l'obiettivo di aumentare notevolmente le proprie *performance*, ma non solo, come meglio si dirà proprio in riferimento alla pubblica amministrazione.

Perché ciò avvenga, è opportuno che istituzioni e imprese interpretino correttamente i dati e che gli stessi siano scambiati in uno spazio digitale sicuro.

Pertanto, con riferimento al primo aspetto, è innanzitutto necessario che i gestori dei dati, siano essi soggetti pubblici o privati, si preoccupino di catturare i dati, computarli e comunicarne i risultati, conformemente alle disposizioni di legge (c.d. "3C" su cui si fonda la *data economy*). Operazione, questa, agevo-

1 Un incentivo all'uso degli strumenti digitali si è avuto proprio nel periodo pandemico, per assicurare servizi pubblici essenziali a distanza, come ad esempio è accaduto per l'istruzione scolastica e la sanità.

2 Z. Baumann, Liquid modernity, Cambridge, 2000 (trad. it. di Sergio Minucci, Modernità liquida, Roma-Bari 2002).

3 L. Torchia, *Lo Stato digitale*, Bologna, Il Mulino, 2023; A Soro, *Persone in rete. I dati fra poteri e diritti*, Fazi editore, 2018.

lata proprio dall'uso di internet, dei sistemi informatici, dalla diffusione a livello mondiale del *Cloud Computing* e della sua integrazione con le reti in ottica *Cloud Integrated Network*[4].

Se correttamente eseguite, tali operazioni dovrebbero permettere lo sviluppo di una "quarta C", che rappresenta la cognizione, ovvero dovrebbero consentire una conoscenza e acquisizione consapevole dei dati che comporti la possibilità, per un'organizzazione o un individuo, di avere sempre più informazioni complete, chiare e rilevanti, per operare in un dato contesto o per il perseguimento di un determinato obiettivo e, quindi, per compiere delle scelte consapevoli[5].

Con riferimento al secondo profilo, invece, ossia quello dell'interoperabilità dei dati in uno spazio digitale sicuro, è evidente che sia necessario un approccio strategico complesso, che si basi: 1) sulla standardizzazione delle procedure e sulla condivisione dei dati e delle informazioni su più livelli; 2) su un necessario coinvolgimento di tutti i settori dell'ordinamento, pubblico e privato[6].

Non a caso, oggi, sempre più spesso si tende a parlare di «Stato digitale»[7] o meglio, di «sovranità digitale», espressione – come chiarito in dottrina – mol-

---

4 Per l'ordinamento italiano si legga: Dipartimento per la trasformazione digitale – Agenzia per la Cybersicurezza nazionale, *Strategia cloud Italia. Documento sintetico d'indirizzo strategico per l'implementazione e il controllo del Cloud della P.A.*, 2021.

5 Sui temi, si veda in dettaglio: *https://www.cloudifynoipa.it/-/data-economy-cos-e-e-come-sfruttarla?inheritRedirect=true*. Cfr. altresì: S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws – Rivista di diritto dei media*, 3/2019, 146 ss.; F. FAINI, Data society. *Governo dei dati e tutela dei diritti nell'era digitale,* Milano, 2019; ID., *Il dato personale tra protezione giuridica e valorizzazione economica*, in *Osservatorio sulle fonti*, 2023, 2.

6 Così: I. FORGIONE, *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in *Dir. amm.*, 2022, 4, 1114 ss.

7 L. TORCHIA, *Lo Stato digitale*, cit.; ma si veda anche: J.B. AUBY, G. DE MINICO, G. ORSONI (diretto da), *L'amministrazione digitale. Quotidiana efficienza e intelligenza delle scelte, Atti del Convegno 9-10 maggio 2022, Federico II, Napoli,* Napoli, Editoriale scientifica, 2023; B. MARCHETTI, *L'amministrazione digitale* (voce), in *Enc. Dir., I Tematici, Funzioni amministrative*, B.G. MATTARELLA, M. RAMAJOLI (diretto da), Milano, 2022; R. CAVALLO PERIN, D.U. GALETTA, *Il diritto dell'amministrazione pubblica digitale*, Torino, Giappichelli, 2020; G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, Giappichelli, 2017.

to spesso utilizzata nella sua accezione più ampia, ricomprendendo in essa non solo tutte quelle funzioni e quei compiti relativi al controllo dei dati in possesso della p.a., bensì anche il controllo delle infrastrutture di rete, dei servizi *cloud* quali vettori per l'uso (e molto spesso abuso) dei dati, non solo da parte del settore pubblico bensì anche – e anzi soprattutto – da parte dei c.d. poteri privati, come sempre più spesso oggi sono qualificate le grandi piattaforme fornitrici di servizi digitali e di rete[8].

E infatti, è stato osservato che proprio l'ascesa delle piattaforme digitali (le c.d. *big five*: Gafam, Google, Apple, Facebook, Amazon E Microsoft) ha notevolmente ampliato il fenomeno della raccolta, gestione e soprattutto della circolazione dei dati, considerata proprio quest'ultima il motore della c.d. *data driven innovation,* tanto da essere stata eletta a quinta libertà fondamentale del mercato unico europeo. Il che con ricadute pesanti sulla tutela dei diritti fondamentali e in particolare sulla tutela dei dati personali[9].

Se questo è il contesto di riferimento, occorre domandarsi quale sia, oggi, il ruolo dello Stato, o meglio, dei pubblici poteri in relazione alla corretta gestione dei dati in un contesto ordinamentale sempre più dematerializzato, digitalizzato, soprattutto a garanzia del delicato equilibrio fra sicurezza, trasparenza e democraticità nel e del trattamento.

2. La gestione dei dati da parte della p.a. e il passaggio dalla logica binaria a quella sistemica

Per rispondere al quesito appena posto, bisogna muovere da alcune considerazioni preliminari.

Ebbene, innanzitutto deve constatarsi che le problematiche relative alla protezione dei dati nel settore pubblico non possano più essere affrontate e ri-

8 O. POLLICINO, Judges, privacy and data protection from a multilevel protection perspective, in *Istituzioni del federalismo*, 2022, 4, 808 ss.; M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, Relazione al Convegno annuale del Gruppo di Pisa, Genova, 18 giugno 2021, consultabile al sito: *www.gruppodipisa.it*.; ID., *I poteri privati nella società digitale: oligopoli e antitrust*, in *Dir. pubbl.*, 2021, 3, 740 ss.

9 L. AMMANNATI, *I «signori» nell'era dell'algoritmo*, in *Dir. pubbl.*, 2021, 2, 381 ss.

solte secondo una logica che chiamerei binaria, ossia secondo una logica meramente individuale o interna, cioè protesa a cogliere il rapporto giuridico bilaterale intercorrente fra titolare del dato e pubblica amministrazione, quale titolare del trattamento – come oggi ampliamente disciplinato dal Regolamento EU n. 679/2016 (d'ora in poi GDPR) –, dovendo piuttosto adottarsi una logica sistemica o trasversale, non solo per l'incalzare di nuove e numerose disposizioni normative, anche europee, che si occupano del tema della gestione dei dati e che impongono una lettura sistematica delle discipline – come meglio si dirà – piuttosto perché i pubblici poteri, oggi, sembrano chiamati a rivestire un nuovo ruolo, diverso e ulteriore rispetto a quello sinora assunto di "mero" titolare del trattamento dei dati[10].

Ciò perché i dati sempre più spesso si caratterizzano per essere non semplicemente declinazione o elemento dei diritti della personalità, piuttosto, beni giuridici dotati di autonoma valenza, come detto, anche economica.

E infatti, sebbene oggi il GDPR costituisca di per sé espressione di una disciplina già avanzata, a tutela del trattamento dei dati personali, sia da parte delle p.a. che dei soggetti privati, cogliendo l'aspetto per così dire dinamico della *privacy*[11], inteso come diritto all'autodeterminazione informativa del singolo, o meglio come diritto al legittimo e lecito/corretto trattamento dei dati, dalla fase della raccolta, gestione, fino alla circolazione del dato stesso[12], la disciplina

10 Sul punto si tornerà oltre, nel tentativo di dimostrare l'assunto.

11 S. Rodotà, *Controllo e privacy della vita quotidiana*, 2009, consultabile al sito www.treccani.it; Id., *Protezione dei dati e circolazione delle informazioni*, Bologna, Il Mulino, 1984; O. Pollicino, F. Resta, *Visibilità del potere, riservatezza individuale e tecnologia digitale. Il bilanciamento delineato dalla Corte*, nota a Corte. Cost. 21 febbraio 2019 n. 20, in *Dir. inf.*, 2019, 110 ss.

12 A mero titolo esemplificativo, sia sufficiente leggere i considerando n. 6, 101, 102 e ss. del Reg. EU n. 679/2016 e poi, in particolare, il Capo V, artt. 44 e 46 ss. in cui la disciplina europea prende in debita considerazione l'ipotesi della circolazione dei dati, avendo ritenuto opportuno assicurare ai dati, scambiati o ceduti in territorio extra-europeo, la stessa protezione assicurata nell'ordinamento interno. Come noto, la disciplina europea ha regolamentato le ipotesi di circolazione dei dati proprio in conseguenza noti casi *Schrems* I e II, di cui si è occupata la Corte di giustizia europea (C. Giust. UE, C-362/2014 e C-311-2018). Con tali sentenze, la Corte di Giustizia EU ha posto le basi per un ulteriore rafforzamento della tutela dei dati e della privacy, valutando l'adeguatezza dei livelli di protezione dei dati, in un contesto digitale, che prevedeva l'uso di piattaforme, e internazionale, essendosi realizzato uno scambio, una cessione di dati oltreoceano. Sui temi: O. Pollicino, Judges, privacy and data protection from a multilevel

in esso declinata appare oggi insufficiente a coprire e a governare integralmente il complesso fenomeno della gestione dei dati.

E ciò per diverse ragioni già evidenziate dalla dottrina[13].

In primis, perché il GDPR sembra cogliere, valorizzare e disciplinare soprattutto la dimensione individuale del dato, nella logica bilaterale del rapporto fra titolare del dato e del trattamento, nella stretta aderenza del dato ai diritti della personalità, alle libertà, alla dignità della persona, a fronte, invece, dell'acuirsi della dimensione per così dire collettiva dei dati, frutto dei processi di anonimizzazione, di aggregazione di dati, che ne enfatizzano la qualificazione degli stessi come autonomo bene giuridico e che al contempo li espongono a usi secondari e a strumentalizzazioni da parte di chi quei dati ha incamerato pur legittimamente[14].

Inoltre perché la logica del consenso, che dovrebbe garantire il legittimo trattamento, molto spesso o si rivela illusoria, per via della forte asimmetria dei mezzi esistente fra individuo e il titolare del trattamento, specie se espressione di un potere privato, o perché è scavalcata dalla necessità di garantire il perseguimento di un interesse pubblico primario, reputato prevalente e come tale capace di sacrificare i diritti dei singoli collegati alla gestione e al trattamento dei propri dati personali[15].

Si può pensare, a tal proposito, alla raccolta massiva di dati per ragioni di sorveglianza, di controllo democratico, di sicurezza urbana[16], o ancora, alla rac-

---

protection perspective, cit.

Per un'analisi approfondita del GDPR, come disciplina avanzata, a tutela della gestione dei dati personali: Circolazione e protezione dei dati personali, tra libertà e regole del mercato: R. Panetta (a cura di), *Commentario al regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice privacy): scritti in memoria di Stefano Rodotà*, Milano, Giuffrè Francis Lefebvre, 2019; O. Pollicino, G. Resta, G. Finocchiaro, R. D'Orazio, *Codice della privacy e della data protection*, Milano, Giuffrè Francis Lefebvre, 2021; G. M. Riccio, G. Scorza - E. Belisario (a cura di), *GDPR e normativa privacy: commentario*, I° ed., Milano, Ipsoa, 2019 e II° ed., Milano, Ipsoa, 2022.

13 Sui temi: L. Torchia, *Lo Stato digitale*, cit., 55 ss.

14 L. Ammannati, *I «signori» nell'era dell'algoritmo*, cit.

15 Da ultimo, quale esempio, si veda: F. Francario, *Il trattamento dei dati personali per finalità di pubblico interesse e l'auspicio di un mutamento d'indirizzo interpretativo*, al sito: *www.giustiziainsieme.it.*

colta di dati biometrici[17]; cosa che porta i sociologi del nostro tempo a parlare di "società" e finanche di "cultura della sorveglianza"[18].

Si deve prendere atto, dunque, che nella società odierna è cresciuta in maniera esponenziale la rilevanza e la dimensione collettiva dei dati, per via dell'implementazione di meccanismi di raccolta di massa di una pluralità di dati dei cittadini (è il caso dei c.d. *big data analytics*, incentivati dall'uso delle tecnologie e degli strumenti d'intelligenza artificiale: si pensi all'uso dei dispositivi IoT – *Internet of things of machines*[19]), nonché l'esigenza di garantire una maggiore interoperabilità[20] dei dati fra istituzioni pubbliche, ma anche fra settore pubblico e privato, non solo per ragioni economiche dettate dal mercato digitale, bensì – come meglio si dirà – anche per finalità altruistiche, a beneficio dell'intera società (si può pensare, ad esempio, all'importanza della condivisione delle informazioni sulla salute del paziente fra operatori sanitari pubblici e privati).

Se questo è il contesto di riferimento, dovrà constatarsi che ai poteri pubblici, oggi, sia attribuito un compito nuovo, d'intermediazione fra individuo, società e mercato nella gestione dei processi di circolazione dei dati, da cui dipen-

16 E. CHITI, *Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia e di difesa*, in *Dir. amm.*, 2016, 4, 511 ss.; S. DEL GATTO, *Quali regole per le nuove tecnologie di riconoscimento facciale? La Corte di Giustizia di Cardiff si pronuncia per la legittimità dell'uso di tecniche di Automated Facial Recognition da parte della Polizia del Galles*, consultabile al sito www.irpa.eu, 2020; ID. E IBIDEM, *Prove di regolazione del riconoscimento facciale e rischi di cattura del regolatore*; nonché *Riconoscimento facciale e diritti fondamentali: quale equilibrio?*, 2020; *Riconoscimento facciale. Secondo uno studio la polizia del Regno Unito nonrispetta gli standard minimi etici e legali,* 2023.

17 Sui rischi correlati alla raccolta di dati biometrici, si veda già: Commissione europea, *Libro bianco sull'intelligenza artificiale*, Bruxelles, COM (2020) 65 final, 19 febbraio 2020.

18 D. LYON, Surveillance society. Monitoring everyday life, Philadelphia 2001 (trad. it. Milano 2002); ma si legga anche: S. RODOTÀ, *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione*, Bari, Laterza, 2004; nonchè S. ZUBOFF, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York, 2019.

19 D.U. GALETTA, *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini?*, in *Ciberspazio e Diritto*, 3/2018; ID., *Open Government, Open Data e azione amministrativa*, in *Istituzioni del federalismo*, 2019, 3, 663 ss.

20 Sulla centralità del processo di interoperabilità organizzativa, tecnica e semantica fra i dati ai fini di una efficiente governance dei dati in un ambiente (recte: ordinamento) digitale, si vedano le Linee guida Agid: "Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni" e le "Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici", ai sensi dell'art. 71 del CAD e della Direttiva (UE) 2015/1535., Determinazione 457/2021 aggiornata con Determinazione 300/2023; nonché ISTAT, Trasformazione digitale della pubblica amministrazione. Metodi per l'interoperabilità per lo sviluppo di *e-service*, Roma, 2023.

de – è questo che si vuole dimostrare – non solo la sicurezza nel trattamento dei suddetti, oltreché la garanzia del bilanciamento fra esigenze di trasparenza o, in senso più lato, di controllo democratico, nonché la tutela dei diritti e delle libertà fondamentali correlate all'uso di quei dati, bensì la garanzia della stessa sicurezza giuridica e ordinamentale.

3. Poteri pubblici e privati nella governance dei dati e nuove esigenze di sicurezza ordinamentale

Le problematiche legate al trattamento dei dati (raccolta, gestione, circolazione) a garanzia del delicato equilibrio fra sicurezza, trasparenza e democraticità nel e del trattamento, impongono l'adozione di un approccio e di una visione sistemica, che richiede di considerare non tanto la distinzione esistente fra tipologie di dati, piuttosto, il differente uso che di tali dati si faccia.

E invero, bisogna rilevare che la distinzione fra categorie di dati (dati personali e non personali, dati aperti, dati suscettibili di essere considerati alla stregua di un bene economico allorché la prestazione del consenso all'utilizzo degli stessi divenga presupposto necessario o, spesso, involontario corrispettivo per la fruizione di servizi, pubblici o privati – si pensi alla profilazione –, sulla base del presupposto che gratuità non sia sinonimo di liberalità) sembra oggi scolorire di rilievo giuridico ai fini di una differenziazione delle discipline di riferimento.

Ciò che sembra emergere dalla lettura sistematica delle discipline normative in vigore[21], è che ci si stia muovendo verso una logica unitaria, che punta a massimizzare e a ottimizzare i benefici economico-sociali che potrebbero derivare dall'utilizzo e dal riutilizzo dei dati, anche personali. Cosa che porta a un sostanziale appaiamento, a un avvicinamento di categorie di dati fra loro molto diverse[22].

21 Si legga, come esempio emblematico, il considerando n. 13 del Reg. UE n. 868/2022 (c.d. *Data governance act*) sul quale ci si soffermerà nel prosieguo.

22 Aa.Vv., *Dati personali. Protezione, libera circolazione e governance*, vol. I, *I principi*, F. Bravo (a cura di), Pacini giuridica, 2023; F. Bravo, *Intermediazione di dati personali e servizi di* «data sharing» *dal GDPR al* «Data Governance act», in *Contratto e impresa Europa*, 2021, 1, 199 ss.

Più interessante, invece, la prospettiva del differente uso che di tali dati s'intenda fare, in quanto tale visuale d'indagine permette di considerare se nella gestione dei dati raccolti prevalga la logica statica, della conservazione, o piuttosto quella dinamica, circolatoria, con ricadute evidenti in tema di sicurezza ordinamentale.

Ebbene. Si ritiene doveroso distinguere nettamente il caso in cui la gestione del dato, specie se personale, sia confinata alla c.d. logica binaria, ossia confinata all'interno di uno specifico rapporto giuridico fra titolare del dato e titolare del trattamento, o piuttosto, assuma rilievo la dimensione esterna ad esso, prevalendo la logica circolatoria e finanche di condivisione dei dati.

A seconda della prospettiva, diverso appare il ruolo della p.a. (o meglio dei pubblici poteri) e diverso il rapporto che viene a configurarsi fra sicurezza, trasparenza e controllo democratico nella gestione dei dati, mutando il rapporto mezzo a fine fra i suddetti principi.

E infatti, nel primo caso (ossia, nella logica binaria) il concetto di sicurezza che sembra venir in rilievo è piuttosto legato a una concezione tradizionale dello Stato, espressione di esigenze di ordine pubblico capaci, in alcune ipotesi, anche di sacrificare, spesso oltremodo, il diritto all'autodeterminazione informativa dei singoli.

Nella logica della raccolta dei dati con finalità di conservazione, la sicurezza pubblica appare il fine ultimo da perseguire, l'interesse primario da garantire, a volte anche a scapito della trasparenza e della tutela dei diritti fondamentali dei singoli (si pensi, ad esempio, all'incremento delle misure e delle prassi di sorveglianza negli aeroporti, nelle città, etc. ...).

Nel secondo caso, invece, quando prevale la logica circolatoria, muta il parametro di riferimento perché il concetto di sicurezza che viene in risalto non è solo quello tradizionale legato alla logica della sovranità statale, piuttosto, è espressione del più moderno concetto di sovranità digitale, di cui si è detto.

Per cui, il valore giuridico di riferimento diviene quello della sicurezza digitale[23], da cui dipendono tanto la tutela della sicurezza (*recte*: della legittimità) nel trattamento dei dati e, dunque, dei diritti fondamentali dei singoli correlati all'uso dei dati, quanto le esigenze di sicurezza pubblica, nella sua logica ordinamentale.

In definitiva, quando a prevalere è la logica circolatoria, sicurezza pubblica e sicurezza nel trattamento dei dati sembrano sublimarsi in un valore giuridico più elevato, quale quello del bisogno di garanzia di sicurezza giuridica che non può che essere assolto se non attraverso il rafforzamento delle esigenze di trasparenza e controllo democratico sulla *governance* dei dati.

Ma vi è di più. Bisogna considerare un ulteriore elemento rilevante, che sembra emergere dalle attuali dinamiche di *governance* dei dati.

In una società che, come constatato, si fa sempre più fluida, liquida, perché deterritorializzata e sempre più dematerializzata, si sta assistendo alla configurazione di nuove dinamiche di potere, in cui i profili di democratizzazione degli stessi diventano difficili da raggiungere.

La configurazione di nuove gerarchie di potere (pensiamo, come detto, all'affermarsi del potere delle grandi piattaforme digitali[24]), che si affiancano ai "tradizionali" poteri pubblici, – i quali, paradossalmente, appaiono oggi più garantisti dei poteri privati, perché per propria natura protesi al doveroso esercizio di un potere, conferito per legge, che non è volto a perseguire finalità egoistiche né lucrative – inesorabilmente, incrementano le disuguaglianze sociali, economiche, digitali, rendendole più difficili da identificare e da colmare[25], pro-

23 Garante per la protezione dei dati personali, *Spazio cibernetico bene comune. Protezione dei dati, sicurezza nazionale*, Atti del Convegno - 30 gennaio 2020, consultabile al sito *www.garanteprivacy.it*.

24 L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. trim. dir. pubbl.*, 2022, 4, p. 1101.

25 Sui divari di cittadinanza presenti nel nostro Paese e sul *digital divide*: F. Panetta, *Lo sviluppo del Mezzogiorno: una priorità nazionale*, www.bancaditalia.it; L. Bianchi, B. Caravita di Toritto (a cura di), *Il PNRR alla prova del sud*, Napoli, Editoriale Scientifica, 2021; A. Barone, *Il tempo della perequazione: il Mezzogiorno nel PNRR*, in *PA – Persona e Amministrazione*, 2/2021; AIPDA – Forum Next Generation EU, con particolare riferimento al *paper* firmato dai Direttori della rivista PA – Persona e Amministrazione: *Diseguaglianze territoriali insostenibili e doveri perequativi inderogabili*, 9 aprile 2021; nonché sia consentito rinviare a: R. Dagostino,

prio perché legate a un contesto deterritorializzato e dematerializzato, che richiede, di conseguenza, nuove forme d'intervento pubblico.

In questo contesto, infatti, i pubblici poteri sembrano atteggiarsi, alla stregua dei singoli individui titolari dei dati, quali soggetti deboli, a fronte del dominio, del potere di alcuni soggetti privati.

Come chiaramente evidenziato in dottrina[26], infatti, nel moderno contesto digitale, appare quantomai opportuno abbandonare la lente deformante della sovranità statale ai fini dell'inquadramento degli istituti e delle figure proprie dell'ordinamento amministrativo, dovendo, oggi, focalizzarsi lo studio del diritto amministrativo, piuttosto in stretta aderenza alle logiche del potere come situazione di asimmetria, a chiunque esso appartenga. Ciò che diviene essenziale è la comprensione delle dinamiche del potere, delle sue fonti di legittimazione, della sua titolarità, delle regole e dei limiti del suo esercizio, dei controlli sulle modalità di estrinsecazione dello stesso. In definitiva, ciò che rileva sono i rapporti fra autorità e libertà nelle dinamiche del potere, nella prospettiva del rafforzamento della logica garantista delle tutele dei cittadini o, meglio, degli utenti, nei confronti dei titolari del potere.

Ciò che traspare è che nella *governance* dei dati, nel moderno ordinamento digitale, siano *nuovamente* (ossia: ancora una volta, bensì anche in maniera innovativa) in gioco i rapporti fra autorità e libertà[27] (individuali ed economiche), che necessitano di un rinnovato bilanciamento.

Sistema delle autonomie e divari territoriali di cittadinanza, Relazione tenuta al XXV Convegno di Copanello "Riflessioni sul diritto amministrativo che cambia", 30 giugno-1° luglio 2023, consultabile anche sulla rivista *Diritto e società*, 2023, 3, 455 ss. si vedano, altresì i seguenti documenti. Banca d'Italia, *Il divario nord-sud: sviluppo economico e intervento pubblico*, giugno 2022; Si leggano anche le delibere della Corte dei Conti sullo stato di avanzamento e di attuazione del PNRR, in particolare: Corte dei Conti, Relazione sullo stato di attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR), marzo 2022; nonché, sulla trasformazione digitale della p.a. e sulla *governance* dei dati, nella prospettiva dell'interoperabilità: Corte dei Conti, sez. controllo, delibera n. 16/2023.

26 L. TORCHIA, *Lo Stato digitale*, cit.

27 Sui rapporti fra autorità e libertà, in generale: AA.VV., *Al di là del nesso fra autorità/libertà: tra legge e amministrazione*, S. PERONGINI (a cura di), Torino, Giappichelli, 2017. In riferimento al tema che si sta affrontando: G. SGUEO, *La visione e la voce nella transizione digitale dei governi democratici*, in *Riv. trim. dir. pubbl.*, 2022, 4, 1015 ss.

4. La strategia europea per i dati

Della complessità ordinamentale sottesa alle nuove dinamiche di potere, che comportano esigenze di rafforzamento della sovranità digitale per l'implementazione di meccanismi efficaci e trasparenti per la *governance* dei dati, sembra essere ben consapevole il legislatore europeo[28] che ha, infatti, di recente messo a punto una vera e propria strategia europea per i dati, basata su un approccio dinamico e trasversale della tutela dei dati, anche personali, perché improntata sulla logica della massima circolazione e finanche della condivisione dei dati, fra settore pubblico e privato.

Particolare importanza rivestono:

1. il Reg. UE 2019/881 sul c.d. *Cybersecurity Act* proteso a garantire la sicurezza cibernetica a livello comunitario, creando un quadro comune per la certificazione informatica dei prodotti e dei servizi digitali, che ha portato, nell'ordinamento interno, alla istituzione di una Agenzia nazionale per la cybersicurezza informatica istituita con Decreto Legge n. 82 del 14 giugno 2021, convertito nella legge n. 109/2021;

2. il Reg. UE 2022/1925 sui mercati digitali (c.d. D.M.A.), volto a regolamentare i rapporti fra imprese che forniscono servizi di piattaforma e imprese che erogano servizi digitali;

3. il Reg. UE 2022/2065 in materia di mercato unico dei servizi digitali (c.d. D.S.A.), proteso a garantire la creazione di un ambiente *on line* sicuro.

Regolamenti, questi ultimi, che prestano particolare attenzione ai dati personali in correlazione alle dinamiche concorrenziali.

4. Si può altresì considerare la proposta di legge, di recente approvata dal Parlamento europeo, relativa al Regolamento europeo sull'intelligenza artificia-

28 Sui temi, si legga il Simposio "*La regolazione digitale nell'Unione Europea*", in *Riv. trim. dir. pubbl.*, 4/2022, e in particolare: B. Carotti, *La politica europea sul digitale: ancora molto rumore*, 997 ss.; M. Libertini, *Il Regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, 1068 ss.; G. Finocchiaro, *La regolazione dell'intelligenza artificiale*, 1085 ss.; L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, cit.; nonché D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2/2023.

le, che stabilisce regole di armonizzazione e particolari obblighi di trasparenza per l'uso di strumenti di intelligenza artificiale per finalità d'interesse generale[29].

5. Infine, ma non ultimo, il Reg. UE 2022/868 sulla Governance europea dei dati (c.d. *Data Governance Act*)[30], che non solo si propone di ampliare le ipotesi di riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici, diversi da quelli aperti, ma offre interessanti novità in materia.

Più in particolare, il *Data Governance Act* si sviluppa lungo quattro direttrici:

1. il riutilizzo di determinati dati detenuti da soggetti pubblici (Capo II),

2. l'attività di intermediazione dei dati[31] (Capo III), tale intendendosi un «servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali a fini di condivisione dei dati tra un numero indeterminato di interessati e di titolari di dati, da un lato, e gli utenti dei dati dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali» (art. 2, par. 1, n. 11).

Il servizio d'intermediazione potrebbe essere svolto anche da servizi di cooperative di dati[32] che avranno il dovere d'informare i titolari del dato sui propri diritti e di assisterlo per effettuare scelte consapevoli sull'utilizzo dei propri dati (art. 2, par. 1, n. 15).

---

29 Si può consultare il testo della proposta di legge approvata dal Parlamento europeo al sito: https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf. Per un primo studio sulla proposta di regolamento europeo sull'intelligenza artificiale, si consulti il sito: https://documenti.camera.it/Leg19/Dossier/Pdf/AT026.Pdf.

30 Tale Regolamento ha completato la disciplina di cui al Regolamento 2018/1807 con cui si era già inteso facilitare lo scambio transfrontaliero dei dati non personali con l'obiettivo di realizzare una economia digitale dei dati più fluida e veloce, pur consentendo alle autorità competenti di richiedere o ottenerne l'accesso in conformità al Diritto dell'Unione Europea o nazionale; nonché la Direttiva 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, inerente i c.d. *open data*.

31 G. Resta, *Pubblico e privato nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, 971 ss.; F. Bravo, *Intermediazione di dati personali e servizi di* «data sharing» *dal GDPR al* «Data Governance act», cit.

32 Sulle cooperative dei dati: F. Bravo, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, 757 - 799.

Non a caso, oggi inizia a parlarsi di neo-mutualismo digitale[33] come modello per lo sviluppo di una economia sociale e solidale a partire dal momento della condivisione e dell'interoperabilità dei dati, non solo fra istituzioni pubbliche, bensì anche fra esse e i privati che si occuperanno di gestire i dati, magari con l'ausilio delle piattaforme digitali o che, come detto, svolgeranno servizio d'intermediazione dei dati.

E infatti, lo scopo sotteso al suddetto regolamento è quello di offrire un quadro normativo armonizzato per lo scambio dei dati nel mercato interno europeo, ponendo gli standard minimi di sicurezza per la *governance* dei dati, prestando particolare attenzione a facilitare la cooperazione tra gli Stati membri. Tale regolamento, quindi, dovrebbe mirare a sviluppare ulteriormente un mercato interno digitale senza frontiere e una società e un'economia dei dati antropocentriche, affidabili e sicure (considerando n. 3).

L'obiettivo, dunque, è quello di realizzare uno spazio amministrativo europeo digitale, sicuro, in cui offrire servizi digitali e definire procedure amministrative uniformi a livello europeo[34], calibrate secondo una prospettiva maggiormente garantista che vede l'utente del servizio al centro (c.d. prospettiva *user-centered*).

3. la messa a disposizione dei dati per fini altruistici, sulla base del principio di solidarietà[35] (Capo IV);

4. l'istituzione di un nuovo sistema di governance dei dati e di sanzioni a fronte di pratiche fraudolente o abusive (Capo V, Capo VI e Capo IX).

---

33 Fondazione Pico, Il manifesto per il neo mutualismo digitale: AA.VV., *Le cooperative e la sfida dell'innovazione digitale: il neo mutualismo in dieci tesi*; A. Baldazzini, *Neo-mutualismo e piattaforme digitali. Intervista a Paolo Venturi*, consultabile al sito *www.pandorarivista.it.*

34 Si prendano come esempi: la creazione di sportelli unici (art. 8 del *Data Governance Act*); la procedura per le richieste di riutilizzo dei dati (art. 9); il Modulo europeo di consenso all'altruismo dei dati (art. 25).

35 F. Bravo, *Il principio di solidarietà*, in *Dati personali. Protezione, libera circolazione e governance*, op. cit., 541 - 601; Id., *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, 405 – 441; Id., *Il principio di solidarietà tra* data protection *e* data governance, in *Il dir. dell'informazione e dell'informatica*, 2023, 3, 481 – 518.

Particolarmente interessante si rivela il profilo dell'altruismo dei dati, di cui al punto 3.

Il regolamento in esame, infatti, definisce «altruismo dei dati»: «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale» (art. 2, par. 1, n. 16).

La condivisione su base volontaria dei dati personali da parte dei soggetti interessati, previo consenso informato, nonchè la condivisione dei dati non personali da parte dei titolari, per finalità d'interesse generale, è valutata dal legislatore europeo come una grande opportunità, una grande potenzialità per la realizzazione di una società sempre più inclusiva, sia socialmente sia economicamente (considerando 45 e 46).

Basti pensare alla condivisione di dati sanitari per finalità di ricerca scientifica, i quali potrebbero tornare utili per indagini di tipo statistico o, in un contesto ancora più evoluto, con l'ausilio di strumenti d'intelligenza artificiale, per consentire l'analisi di tali dati attraverso modalità di apprendimento automatico.

È evidente, pertanto, che queste nuove disposizioni normative si saldino e completino la disciplina sulla gestione dei dati di cui al GDPR, implementando considerevolmente non solo la logica della circolazione dei dati, bensì anche quella dell'interoperabilità fra settore pubblico e privato, nonché quella, ancor

più innovativa, della condivisione dei dati, anche personali, in chiave solidaristica.

Purtuttavia, è opportuno che la creazione di questo ecosistema digitale basato su dati interdipendenti, ossia sulla circolazione, sull'interoperabilità fra settore pubblico e privato, sulla condivisione altruistica dei dati medesimi, si dispieghi in un contesto ordinamentale sicuro, in cui le garanzie di effettività delle regole e delle tutele[36] siano realmente in grado di far crescere la fiducia dei cittadini nei confronti di tali poteri, in relazione ai servizi forniti per la *governance* dei dati.

5. L'implementazione dell'apparato organizzativo e delle funzioni di amministrazione attiva per la governance dei dati in un ordinamento digitale sicuro e solidale

L'esigenza di garantire una maggiore interoperabilità dei dati fra settore pubblico e privato, non solo per ragioni economiche dettate dal mercato digitale, bensì per finalità altruistiche, solidaristiche, a beneficio della società, del progresso sociale, richiede rinnovate forme di interventismo pubblico nella realtà economica, sociale e digitale, aumentando i rischi in relazione a un sistema di gestione dei dati, che appare molto più complesso.

Il legislatore europeo, infatti, nel delineare la strategia europea per i dati, implementandola anche con l'innovativo principio dell'altruismo dei dati, funzionale al perseguimento di obiettivi di interesse generale, si è preoccupato di implementare l'apparato amministrativo europeo per la *governance* dei dati, sia per il profilo organizzativo sia per quello funzionale, in una prospettiva che non è semplicemente quella, pur imprescindibile, dell'armonizzazione delle procedure e degli standard qualitativi di prestazione di servizi digitali, piuttosto quella più pregnante di realizzare un ecosistema (*recte*: un ordinamento) digitale europeo sui dati quanto più uniforme, sicuro, garantista.

---

36 G. CORSO, M. DE BENEDETTO, N. RANGONE, *Diritto amministrativo effettivo*, Il Mulino, Bologna, 2023, p. 51 ss.

Se si legge il *Data Governance Act* ci si avvede subito che a fronte di un'apparente liberalizzazione nella gestione dei dati, non solo attraverso la valorizzazione dell'apporto degli operatori privati nei servizi d'intermediazione dei dati, bensì attraverso il riconoscimento al singolo individuo di più ampi margini decisori in relazione ai propri dati, essendo ormai legittimato a compiere atti di liberalità sui propri dati personali, disponendo degli stessi, previo consenso informato, per finalità altruistiche[37], sono state notevolmente rafforzate le forme di intervento pubblico per la *governance* dei dati.

Più particolare, pare si vada verso una sicura implementazione:

- sia dell'apparato organizzativo pubblico, essendo ad esempio prevista:

i. la possibilità di istituire sportelli unici (art. 8) che fungano da interfaccia per i riutilizzatori dei dati, ossia i fornitori di servizi di *data sharing* – cioè i servizi d'intermediazione dei dati (c.d. infomediari[38]);
ii. l'istituzione di organismi di supporto agli enti pubblici che dovrebbero agevolare la circolazione e condivisione dei dati, ossia le c.d. strutture di assistenza che dovrebbero operare conformemente alle istruzioni ricevute dall'ente pubblico (considerando 26);
iii. l'istituzione di Autorità competenti per i servizi di intermediazione dei dati (art. 13);
iv. l'istituzione di Autorità competenti alla registrazione delle organizzazioni per l'altruismo dei dati (art. 23)

- sia dell'esercizio di funzioni di amministrazione attiva, incombendo sui pubblici poteri nuovi compiti a garanzia della tutela dei diritti dei singoli correlati all'uso e alla gestione dei dati personali. Si pensi, ad esempio, alla predisposizione di condizioni

37 Cosa che ha portato anche al riconoscimento di nuove figure soggettive; ad esempio, accanto al titolare del dato, si delinea la nuova figura "dell'utente" del dato, quale persona fisica e giuridica che ha accesso legittimo a dati altrui, personali e non (si vedano le definizioni di cui all'art. 2 del regolamento)

38 F. BRAVO, *Intermediazione di dati personali e servizi di* «data sharing» *dal GDPR al* «Data Governance act», cit.

per il riutilizzo dei dati (art. 5 del regolamento); alla possibilità di predisporre tariffe per il riutilizzo dei dati (art. 6); alla definizione di procedure per la richiesta di riutilizzo dei dati (ai sensi dell'art. 9); alla predisposizione di misure tecniche e organizzative per garantire l'altruismo dei dati (art. 16 ss.); all'imposizione di obblighi di trasparenza (art. 20).

Inoltre, dall'analisi complessiva del "pacchetto regolatorio" predisposto dall'UE emerge il potenziamento della funzione di regolazione, attraverso l'adozione di un approccio regolatorio nuovo, che valorizza la logica *ex ante*, basata sulla gestione precauzionale dei rischi.

Ciò porta alla valorizzazione dell'esercizio della funzione di vigilanza[39], quale funzione di amministrazione attiva, che si esercita *ex ante* e in maniera continuativa (c.d. *ongoing*), ossia che si svolge senza soluzione di continuità e in maniera concomitante all'esercizio dell'attività privata vigilata, sia essa economica o di rilievo solidaristico che, nel caso di specie, impone una valutazione di adeguatezza sui livelli di protezione prescelti nei modelli contrattuali che predefiniscono le condizioni di utilizzo, gestione, circolazione e condivisione dei dati, nonché sulle modalità di protezione che s'intendono predisporre a garanzia dei diritti sui dati e finanche un'attività di assistenza ai riutilizzatori dei dati (5 Reg. UE 2022/868). Quindi, una funzione che implica un'attività di *tutorship*[40] da parte delle autorità pubbliche nei confronti dei privati che operano come intermediari o che si inseriscono come soggetti attivi in questo complesso ma unita-

39 L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, cit. Sulla centralità e rilevanza che la funzione di vigilanza sta acquisendo anche in altri settori dell'ordinamento, come quello bancario, si vedano: A. Barone, G. Drago, *La funzione di vigilanza della Banca Centrale Europea. Poteri pubblici e sistema bancario*, LUISS University Press, Roma, 2023; M.P. Chiti, V. Santoro, *L'Unione Bancaria Europea*, Pisa, Pacini Giuridica, 2016; M. Macchia, *Integrazione amministrativa e unione bancaria*, Torino, Giappichelli, 2019; A. Magliari, *Vigilanza bancaria e integrazione amministrativa europea. Profili di diritto amministrativo*, Trento, 2020; nonché sia consentito rinviare altresì a: R. Dagostino, *Vigilanza bancaria e stabilità sistemica*, Napoli, Edizioni Scientifiche Italiane, 2023.

40 Sul punto, più approfonditamente: R. Dagostino, *Vigilanza bancaria e stabilità sistemica*, cit.

rio processo di gestione, circolazione, condivisione dei dati, basato sull'interoperabilità dei dati medesimi.

Funzione, quella di vigilanza, che oggi sempre di più tende a delinearsi come funzione dotata di autonoma valenza giuridica, meritevole di riconoscimento in una categoria giuridica autonoma, non compendiabile nel più lato concetto di regolazione, né men che meno nella funzione di controllo-sanzione, rispondente alla diversa logica dell'intervento pubblico *ex post*.

E di tanto si trova conferma nello stesso Reg. EU 2022/868, in particolare nel considerando 26, negli artt. 13 e 14 nonché negli artt. 23 e 24 lì dove il legislatore europeo suggerisce che la funzione di vigilanza nella *governance* dei dati, ai fini dell'autorizzazione al riutilizzo e alla intermediazione dei dati, non dovrebbe esser svolta da quei soggetti competenti all'esercizio della funzione di controllo.

Si prevede, infatti, la possibilità di istituire Autorità competenti per i servizi di intermediazione dei dati, nonché Autorità competenti alla registrazione delle organizzazioni per l'altruismo dei dati, le quali sono chiamate a svolgere funzioni di monitoraggio delle conformità, dunque di vigilanza, le quali dovranno, piuttosto, cooperare con le autorità preposte al controllo sul trattamento dei dati, dando vita a un vero e proprio *network* fra i pubblici poteri ai fini dell'efficiente ed effettiva *governance* dei dati.

6. Sicurezza, trasparenza, solidarietà e democrazia: quale ruolo per i pubblici poteri?

La strategia europea per i dati, così come delineata, mostra chiaramente che i pubblici poteri siano tenuti ad adottare un approccio di tipo proattivo, *in primis*, mediante il rafforzamento della *governance* dei dati e della gestione dei rischi correlati, essendo chiamati a implementare l'apparato organizzativo pubblico e le funzioni di amministrazione attiva, a garanzia della legittima gestione (raccolta, uso, riutilizzo, circolazione, condivisione) dei dati.

Si è evidenziato, infatti, che s'intravedono chiaramente nuovi scenari d'intervento pubblico ai fini del trattamento, della gestione, della circolazione dei dati, con conseguente possibile implementazione dell'apparato amministrativo e rafforzamento dell'esercizio di funzioni non solo di regolazione, controllo e sanzione, bensì verosimilmente, anche di amministrazione attiva, a garanzia di un difficile equilibrio fra sicurezza, trasparenza e solidarietà.

Ancora, sebbene non emerga immediatamente dalla regolazione in questione, bensì da una interpretazione sistematica delle normative in vigore sopra richiamate, è altresì evidente che i pubblici poteri siano chiamati a uno sforzo ulteriore, quello che chiameremmo la sfida delle competenze, dovendo necessariamente garantire l'interoperabilità fra i dati, sia fra le medesime istituzioni, sia fra esse e gli operatori privati, in specie i gestori delle piattaforme o coloro che svolgeranno servizi di intermediazione, mediante l'ausilio di strumenti digitali.

Infatti, il processo di trasformazione digitale della p.a. deve essere inteso come passaggio necessario per implementare i meccanismi di *good governance* and *social accountability*, essendo proteso a garantire il superamento del *digital* divide esistente in Italia che, di fatto, compromette l'effettività dell'azione amministrativa e l'erogazione di servizi pubblici essenziali nei contesti in cui il rapporto giuridico amministrativo risulti dematerializzato.

Di tanto si trova chiara conferma anche nel Piano nazionale di ripresa e resilienza (PNRR), in particolare con riferimento all'investimento 1.3. "Dati e interoperabilità", teso a promuovere le modalità di interconnessione tra le basi dati delle Amministrazioni, onde creare una "Piattaforma Digitale Nazionale Dati".

Investimento declinato proprio all'interno della più generale Missione n. 1, dedicata alla digitalizzazione della p.a., in cui si evidenzia che «la parabola verso l'innovazione tecnologica del Paese non può prescindere da una piena interoperabilità tra le risorse informative degli enti pubblici, che "consenta di snellire le procedure pubbliche grazie alla piena realizzazione del principio (e

obiettivo/standard della CE) del "*once only*", un concetto di *e-government* per cui cittadini e imprese debbano poter fornire "una sola volta" le loro informazioni ad autorità ed amministrazioni"».

In questa cornice, dunque, necessariamente si inquadra la *governance* dei dati.

Ma vi è di più. Al di là delle questioni prettamente organizzative o di amministrazione attiva, un problema ben più complesso è emerso.

Nella volontà di ristabilire un nuovo equilibrio fra poteri pubblici e privati o, meglio, fra autorità e libertà, sembra che a venire in discussione non sia "soltanto" o "semplicemente" il bisogno di sicurezza, inteso in senso lato, come sicurezza/certezza giuridica, che passa anche attraverso il rafforzamento degli obblighi di trasparenza[41] (si vedano, ad esempio, il considerando n. 52 e l'art. 20 *del Data Governance Act* che pongono un collegamento diretto fra sicurezza giuridica e trasparenza), o ancora, la definizione di standard di adeguatezza nel trattamento dei dati, essendo i titolari del trattamento dei dati tenuti ad adottare tutte le misure organizzative necessarie per una corretta gestione dei dati medesimi, piuttosto, un ripensamento del concetto stesso di sovranità.

In un contesto sempre più deterritorializzato, dematerializzato e ibrido, in cui i confini fra poteri pubblici e privati si fanno labili, essendo essi chiamati a cooperare fra loro nella gestione dei dati (dando vita a una vera e propria co-regolazione[42] e co-gestione) è opportuno che le istituzioni pubbliche assicurino quel delicato equilibrio fra sicurezza, trasparenza e democraticità nel e del trattamento dei dati.

I pubblici poteri cioè devono farsi garanti della democrazia[43] digitale.

---

41 F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. inf.*, 2015, 227 ss.

42 Parla di co-regolazione A. SIMONCINI, *La co-regolazione delle piattaforme digitali,* in *Riv. trim. dir. pubbl.*, 2022, 4, 1031 ss.; ma si veda anche, IBIDEM: O. POLLICINO, *I codici di condotta tra* self-regulation *e* hard law*: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione* online, p. 1051. Si v. altresì: E. BRUTI LIBERATI, *Poteri privati e nuova regolazione pubblica*, in *Dir. pubbl.*, 1/2023.

43 Più in generale, sulla costruzione di una società democratica europea, si veda il Simposio "*Il cambiamento strutturale del diritto pubblico europeo*", in *Riv. trim. dir. pubbl.*, 3/2023.

A loro l'arduo compito di assicurare non semplicemente una adeguata protezione dei dati personali, bensì una equivalenza sostanziale nella gestione dei dati, nell'interoperabilità dei dati fra istituzioni pubbliche, nonché fra loro e i privati, in un contesto dematerializzato in cui, lo si è visto, a mutare è il concetto stesso di sovranità.

Ai poteri pubblici, dunque, è attribuito un delicato compito d'intermediazione fra individuo, società e mercato nella gestione dei processi di circolazione dei dati, da cui dipende non solo la sicurezza nel trattamento dei suddetti, bensì la garanzia della stessa sicurezza giuridica e ordinamentale.

Nel farsi garanti della democrazia digitale, agli stessi il compito di farsi promotori, nell'esercizio delle proprie funzioni, di un approccio non solo *user-centered*, come detto fondamentale per la definizione di procedure uniformi a livello europeo, a garanzia della fruizione di servizi digitali collegati alla gestione dei dati, rispettosi di standard qualitativi minimi, bensì di un approccio che potrebbe definirsi *community-centered*, ossia teso a incentivare processi collaborativi virtuosi in una società, o meglio, in un ordinamento complesso che vede una pluralità di attori – poteri pubblici, poteri privati, siano essi operatori economici o singoli individui capaci di disporre dei propri dati –, al fine di migliorare l'efficacia e la sostenibilità delle azioni per costruire comunità sane, che incoraggino l'equità, la connessione sociale, la solidarietà.
In una sola parola, la democraticità dell'ordinamento giuridico tutto.