L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali

Mario Midiri e Simona Piva *

SOMMARIO: 1. I compiti d'interesse pubblico tra Regolamento UE e legislazione nazionale: discrezionalità degli Stati e principio di coerenza. – 2. I principi delineati dal GDPR. – 3. Pluralità degli interessi pubblici e loro bilanciamento. – 4. Interesse pubblico e trattamento dei dati negli artt. 2-*ter*, 2-*sexies* e 2-*quinquiesdecies*, Codice. – 5. Comunicazione e diffusione dei dati: base giuridica. – 6. Circolazione dei dati e pubblici poteri nella *digital society*.

1. *I compiti d'interesse pubblico tra Regolamento UE e legislazione nazionale: discrezionalità degli Stati e principio di coerenza*

Sin dal Considerando 10, il GDPR chiarisce la *ratio* ispiratrice della nuova normativa. La protezione delle persone fisiche a un livello «coerente ed elevato» coesiste con l'obiettivo di rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il che richiede *standard* di protezione equivalenti in tutti gli Stati membri [1]. Questa esigenza vale anche al momento di definire la sfera degli obblighi legali e dei compiti d'interesse pubblico: la garanzia dei beni giuridici d'interesse pubblico deve salvaguardare il principio di proporzionalità, declinato nei tre profili messi in luce dalla giurisprudenza eurounitaria [2].

---

* Gli Autori hanno discusso e condiviso l'intero testo. I parr. da 1 a 3 sono comunque da ascrivere a M. Midiri; quelli da 4 a 6 a S. Piva.

[1] La premessa economica consiste nel peso della circolazione dei dati nel mercato interno europeo: l'aumento della facilità di circolazione dei dati personali richiede un "cambio di rotta" per assicurare un contesto normativo affidabile per gli operatori economici, favorevole alla crescita *data driven*: C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello*, Ed. scientifica, Napoli, 2018, pp. 43 ss.; G. FINOCCHIARO, *Introduzione* al *regolamento europeo sulla protezione dei dati personali*, in *Nuove leggi civ. comm.*, 2017, p. 2, e, per un confronto con l'assetto normativo previgente, ID., *Privacy e protezione dei dati personali*, Zanichelli, Bologna, 2012.

[2] Sui tre distinti profili del principio: *idoneità* – rapporto tra il mezzo adoperato e l'obiettivo perseguito. In virtù di tale parametro l'esercizio del potere è legittimo solo se la soluzione adottata consenta di raggiungere l'obiettivo; *necessarietà* – assenza di qualsiasi altro mezzo

Nella definizione degli interessi pubblici rilevanti, il Regolamento definisce una cornice generale, ma agli Stati membri è riconosciuta una parziale autonomia normativa, tanto che si parla di potestà statale integrativa [3].

Il buon funzionamento del mercato unico richiede, invero, che lo "spazio di manovra" degli Stati membri [4] sia rispettoso del principio di coerenza. Questo principio è presidiato da meccanismi di raccordo in fase applicativa grazie alla "rete" delle Autorità garanti e al ruolo svolto dall'*European Data Protection Board* (GDPR, artt. 68 e seguenti) [5].

---

idoneo ma tale da incidere in misura minore sulla sfera del singolo In virtù di tale parametro la scelta tra tutti i mezzi astrattamente idonei deve cadere su quella che comporti il minor sacrificio; *adeguatezza* – tollerabilità della restrizione per il privato: l'esercizio del potere, pur idoneo e necessario, è legittimo solo se rispecchia una ponderazione bilanciata degli interessi. Sul principio di proporzionalità, Corte giust., sent. 29 novembre 1956, causa 8/55, *Fédéchar* e sopratt. sent. 17 dicembre 1970, in causa 11/70, *Internationale Handelsgesellschaft*; v. poi sentt. 11 luglio 1989, causa 265/87, *Schräder*; 13 novembre 1990, causa 331/88, *Fedesa*, in *Racc.*, 1990, 4023 e del 5 ottobre 1994, causa C-133/93, C-300/93 e C-362/93, *Crispoltoni et al.*, in *Racc.*, 1994, 4863; v. anche le conclusioni dell'Avv. Gen. Stix-Hackl nel caso *OMEGA* (Corte giust. CE, sentenza del 4 ottobre 2004, in causa C-36/02, in *Racc.*, 2004, 9609). Cfr., inoltre, sull'effetto di *spill over*, D.U. Galetta, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Giuffrè, Milano, 1998.

[3] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, *Il Regolamento europeo 2016/679*, II, Giappichelli, Torino, 2016, pp. 17 ss.; S. D'Ancona, *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo*, in *Riv. it. dir. pubbl. com.*, 2018, pp. 587 ss.; cfr., pure, F. Di Resta, *La nuova "privacy europea". I principali adempimenti del Regolamento UE 2016/679 e profili risarcitori*, Giappichelli, Torino, 2018; E. Pelino, C. Bistolfi, L. Bolognini, *Il Regolamento Privacy europeo: commentario alla nuova disciplina europea sulla protezione dei dati in vigore da maggio 2016*, Giuffrè, Milano, 2016; C. Kuner, L.A. Bygrave, C. Docksey, *Commentary on the EU General Data Protection Regulation*, *Oxford University Press*, 2018. I meccanismi di raccordo procedurale sembrano in grado di limitare il rischio che l'autonomia normativa degli Stati comprometta l'uniformità di applicazione del regolamento: su tale pericolo, v. F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ.*, 2017, 2, pp. 369 ss.

[4] Sul ruolo di specificazione affidato alle fonti dello Stato membro v., fin d'ora, l'art. 2-*sexies*, Codice.

[5] Il *Board* ha sostituito il vecchio Gruppo dei Garanti europei, istituito dall'art. 29 della direttiva 95/46, abrogata dal GDPR. Sul principio di coerenza, v. l'art. 63 GDPR, *Meccanismo di coerenza*: «Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione». Per un esempio di pronuncia del *Board* v. la *Opinion 12/2018* (*on the draft list of the competent supervisory Authority of Italy regarding the processing operations subjects to the requirement of a data protection impact assessment*), adottata in applicazione dell'art. 64 GDPR, che prevede il parere del Comitato sul progetto di decisione sull'elenco di trattamenti soggetti a valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, par. 4.

2. *I principi delineati dal GDPR*

È da considerare innanzitutto la cornice istituzionale definita dal GDPR.

1) L'art. 9 GDPR, al primo paragrafo, elenca i dati personali c.d. "sensibili" (ivi includendo i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, ed anche i dati genetici e biometrici, i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona). Vale per questi dati un tendenziale divieto di trattamento. Ma anche per queste categorie particolari è dato specifico rilievo ai "motivi d'interesse pubblico". L'art. 9 GDPR consente, infatti, di non applicare il divieto di trattamento dei dati particolari (oltre al caso in cui vi sia consenso o sussista l'interesse della persona) quando il trattamento sia necessario per l'esercizio della funzione giurisdizionale e per la tutela di un diritto in sede giudiziaria (v. la lett. *f*) e qualora vi siano esigenze sanitarie, di medicina del lavoro e di prevenzione (v. lett. *h*) e *i*), di archiviazione nel pubblico interesse, di ricerca o fini statistici (v. lett. *j*).

L'art. 9, par. 2, lett. *g*), contiene, poi, una clausola di rinvio alla legislazione degli Stati membri (v., da noi, l'art. 2-*sexies* Codice) per identificare i motivi d'interesse pubblico, sempre nel rispetto del canone di proporzionalità rispetto alla finalità perseguita e con la garanzia del diritto alla protezione dei dati personali.

2) Specifica rilevanza hanno le esigenze di sicurezza, anche a fini di prevenzione, e le indagini giudiziarie[6]. Anche qui si deve, però, rispettare il principio di proporzionalità[7]. Questo è un punto fermo della giurisprudenza eurounitaria, che trova conferma nell'art. 52, par. 1, della Carta dei diritti fondamentali: le limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono essere compatibili con il contenuto essenziale di detti diritti e rispettare il principio di proporzionalità: esse possono essere adottate «solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui»[8].

---

[6] In base all'art. 2, par. 2, lett. *d*), GDPR, il regolamento non si applica ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse. Cfr., pure, l'art. 10 GDPR (trattamento dei dati personali relativi a condanne e reati). In dottrina si è aperto un dibattito interessante sulla qualificazione del "diritto alla sicurezza" come base necessaria per assicurare l'esercizio degli altri diritti costituzionali; in questo senso si tratterebbe di un diritto costituzionale "superprimario": cfr. G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi cost.*, n. 3, 2008. Non sarebbero, però, giustificate restrizioni a libertà fondamentali non adeguate e non necessarie: netta è su questo la giurisprudenza della Corte del Lussemburgo, su cui v. le note che seguono.

[7] C. COLAPIETRO, *op. cit.*, p. 61.

[8] Si veda, in part., la sentenza 8 aprile 2014 della Corte di giustizia UE, Grande Sezione, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e a.*, di cui, soprattutto, i par. 38 ss. La Corte, in questo caso, si è pronunziata su due domande di pronuncia pregiudiziale, presentate rispettivamente dalla *High Court* dell'Irlanda e dal *Verfassungsgerichtshof* au-

Va altresì sottolineato – ma è punto che qui si può solo accennare – che il rilievo dato dal GDPR alle esigenze di sicurezza porta con sé il problema della diversa estensione di tale figura nei diversi Stati membri, il che ha una evidente ricaduta sulle concrete modalità applicative della normativa di protezione dei dati [9].

In conclusione, si può affermare che il Regolamento UE 2016/679 pone dunque un quadro sufficientemente elastico, affinché il legislatore nazionale possa specificare ulteriormente gli interessi pubblici rilevanti, come avvenuto con gli artt. 2-*ter*, 2-*sexies* e 2-*quinquiesdecies*, d.lgs. 30 giugno 2003, n. 196, nel testo modificato dal d.lgs. 10 agosto 2018, n. 101: tali disposizioni affermano – fuori dalle particolari categorie dell'art. 9 GDPR – il principio di tipizzazione dei casi di comunicazione, con riserva di legge o di regolamento autorizzato, e con una clausola finale permissiva della comunicazione necessaria allo svolgimento di "compiti di interesse pubblico e di funzioni istituzionali", previa notifica al Garante e con previsione del silenzio assenso del Garante stesso.

3. *Pluralità degli interessi pubblici e loro bilanciamento*

Nell'individuare la gamma degli interessi pubblici rilevanti, occorre dunque tenere sempre ben presente l'intreccio tra la fonte di diritto UE immediatamente esecutiva (il GDPR) e la legislazione nazionale: il contestuale esame di questi due

striaco, aventi ad oggetto la validità della direttiva 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, che modifica la direttiva 2002/58/CE. La Corte ha dichiarato la direttiva 2006/24/CE invalida, rilevando che la direttiva riguarda qualsiasi persona e mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi; essa non prevede alcun criterio oggettivo né le condizioni sostanziali o procedurali che permettano di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore; la direttiva impone un periodo di conservazione dei dati di sei mesi ma non effettua alcuna distinzione tra le categorie di dati a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate e non determina la durata di conservazione in base a criteri obiettivi al fine di garantire che sia limitata allo stretto necessario. Dal momento che la direttiva non impone che i dati siano conservati sul territorio dell'Unione, non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, richiesto dall'art. 8, comma 3, della Carta dei diritti fondamentali UE. Risultano quindi oltrepassati i limiti imposti dal rispetto del principio di proporzionalità alla luce degli artt. 7, 8 e 52, comma 1, della Carta. La direttiva non realizza un corretto bilanciamento tra la necessità di garantire la sicurezza pubblica contro la criminalità grave, attraverso la conservazione dei dati personali nell'ambito delle comunicazioni elettroniche, e il diritto dei cittadini alla protezione dei dati personali, sotto il profilo del diritto fondamentale al rispetto della vita privata.

[9] Già si pone la questione dell'ammissibilità di tecniche di *Artificial Intelligence* come il riconoscimento facciale da parte delle Forze di Polizia: le esigenze di sicurezza "sbarrano la strada" all'applicazione delle norme di garanzia del GDPR, e la diversa conformazione degli ordinamenti statali in punto di sicurezza lascia aperto un possibile divario discrezionale tra gli Stati su cui è bene interrogarsi.

livelli di produzione normativa (e di contestuale elaborazione giurisprudenziale) giova a superare l'antica questione della indeterminatezza del concetto di *interesse pubblico*[10]. Questione che ha sollecitato l'attenzione sia sul profilo diacronico, per le conseguenze giuridiche prodotte dall'evoluzione sociale (cui fa riscontro un diverso assetto dei poteri amministrativi per far fronte al mutare dei bisogni), sia su quello sincronico, per l'eterogeneità degli interessi pubblici meritevoli di protezione[11].

Le occasioni di bilanciamento tra i plurimi interessi in conflitto – si pensi alla tensione tra il diritto alla privacy[12] e le esigenze di sicurezza pubblica – possono dare invero uno spazio assai ampio (e non facilmente controllabile) al potere di scelta discrezionale dell'amministrazione. Ma sovvengono a rimedio i "grandi principi" elaborati dalla giurisprudenza europea e dalle Corti costituzionali nazionali: il principio di proporzionalità e il rispetto del contenuto essenziale del diritto. Principi entrambi richiamati, come si è visto, dal GDPR. Ed ancora, il principio di legalità e la previsione di specifiche riserve di legge impongono la predeterminazione dei poteri e delle modalità dell'azione amministrativa[13], anche in vista della necessaria garanzia dei diritti degli interessati[14] e del controllo giurisdizionale pieno ed effettivo postulato dagli artt. 24 e 111 Cost.

---

[10] V., in part., M.S. GIANNINI, *Istituzioni di diritto amministrativo*, 2ª ed. aggiornata a cura di A. MIRABELLI CENTURIONE, Giuffrè, Milano, 2000, p. 22: «La categoria meno definibile è […] quella degli interessi pubblici».

[11] Sull'interesse pubblico come entità dinamica e dialettica, V. CERULLI IRELLI, *Lineamenti di diritto amministrativo*, Giappichelli, Torino, 2012, pp. 283 ss. Sull'importanza della sede procedimentale come "luogo" in cui gli interessi pubblici rilevanti assumono concretezza, F.G. SCOCA, M.R. SPASIANO, *Nozioni introduttive*, in F.G. SCOCA (a cura di), *Diritto amministrativo*, Giappichelli, Torino, 2011, 3ªed., pp. 15 ss. Sull'evoluzione del concetto di interesse pubblico (e del correlato concetto di potere pubblico): A. PIZZORUSSO, *Interesse pubblico e interessi pubblici*, in *Riv. trim. dir. pubbl.*, 1972, pp. 85-87; F. RANGEON, *L'idéologie de l'intéret general*, Éditions Economica, Paris, 1986. Sul rilievo che assume l'individuazione di un centro organizzativo pubblico, già esistente ovvero appositamente creato, che viene preposto alla cura dell'interesse, v. M. CLARICH, *Manuale di diritto amministrativo*, il Mulino, Bologna, 2013, 3ªed., pp. 95 ss.; M.S. GIANNINI, *op. cit.*, p. 24; M. MERLONI, *Istituzioni di diritto amministrativo*, Giappichelli, Torino, 2012, p. 4.

[12] La protezione dei dati personali è un diritto che l'Unione europea ha messo al centro della sua azione a partire dalla Carta dei diritti fondamentali dell'Unione europea o Carta di Nizza, proclamata nel 2000 a Nizza e, una seconda volta, in una versione modificata, nel 2007 a Strasburgo, che all'art. 8, par. 1, sancisce che «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». Un'ampia ricognizione sul fondamento costituzionale del diritto alla riservatezza e delle modalità del suo bilanciamento in S. SCAGLIARINI, *La riservatezza e i suoi limiti*, Aracne, Roma, 2013. Sulla privacy come sommatoria di tre distinti diritti: il diritto alla riservatezza, il diritto all'identità personale e, per l'appunto, il diritto alla protezione dei dati personali, v. J.L. A BECCARA, *La privacy nel pubblico. Sintesi dell'integrazione tra Codice italiano e Regolamento europeo per la Pubblica amministrazione*, Franco Angeli, Milano, 2018, p. 17.

[13] M. CLARICH, *op. cit.*, p. 107.

[14] F. PIRAINO, *op. cit.*, pp. 369 ss.

4. *Interesse pubblico e trattamento dei dati negli artt. 2-ter, 2-sexies e 2-quinquiesdecies, Codice*

Analizziamo ora gli artt. *2-ter*, *2-sexies* e *2-quinquiesdecies*, d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101.

L'art. *2-ter* riguarda la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri. Esso "riprende" l'art. 19 del previgente *Codice in materia di protezione dei dati personali*, d.lgs. 30 giugno 2003, n. 196, il cui ambito di applicazione soggettivo viene esteso al fine di recepire l'impostazione adottata dal Regolamento [15].

La distinzione basata sulla natura pubblica o privata dei soggetti che trattano i dati è accantonata: ciò che rileva è la finalità del trattamento perseguita. La disposizione si applica a tutti i soggetti che trattano i dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a prescindere dalla loro natura soggettiva (art. 6, par. 1, lett. *e*), GDPR).

La base giuridica per il trattamento dei dati, individuata ai sensi dell'art. 6, par. 3, lett. *b*), GDPR, è costituita a livello nazionale «esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento» (art. *2-ter*, comma 1): l'identificazione degli interessi pubblici avviene in base alla legge [16].

Sono introdotte specifiche condizioni di ammissibilità riguardanti «la comunicazione fra titolari che effettuano trattamenti personali» (art. *2-ter*, comma 2) [17] e «la diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità» (art. *2-ter*, comma 3) [18].

Il comma 2 ammette la comunicazione di dati personali, «diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'art. 10 del Regolamento», fra Pubbliche Amministrazioni non solo se prevista ai sensi del comma 1, ma anche in assenza di una specifica fonte di legittimazione, purché siano compresenti tre condizioni:

a) la comunicazione avvenga fra titolari che effettuano trattamenti di dati personali;

---

[15] Cfr. M. Iaselli, *In G.U. il decreto di adeguamento al GDPR*, in *Quot. giur.*, 5 settembre 2018, *http://www.quotidianogiuridico.it/documents/2018/09/05*.

[16] V. Cerulli Irelli, *op. cit.*, p. 345.

[17] Mentre la comunicazione di dati personali tra privati è vincolata al consenso dell'interessato, la comunicazione tra amministrazioni, «in considerazione della elevata potenzialità lesiva, richiede una specifica "norma di legge o di regolamento" che autorizzi questa specifica tipologia di trattamento»: S. D'Ancona, *op. cit.*, p. 597.

[18] «Le richieste di comunicazione inviate dalle autorità pubbliche dovrebbero sempre essere scritte, motivate e occasionali e non dovrebbero riguardare un intero archivio o condurre all'interconnessione di archivi. Il trattamento di tali dati personali da parte delle autorità pubbliche dovrebbe essere conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento»: Considerando 31, GDPR.

b) la comunicazione sia comunque necessaria per lo svolgimento di un compito di interesse pubblico e lo svolgimento di funzioni istituzionali;

c) sia stata effettuata comunicazione all'Autorità di controllo, ossia al Garante per la protezione dei dati personali, della necessità della comunicazione per i fini *supra* richiamati al punto b) ed il Garante, decorso il termine di quarantacinque giorni, non abbia espresso il suo diniego sulla possibilità della comunicazione o non abbia date precise prescrizioni a tutela degli interessati[19].

Il comma 3 prevede che la diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità, siano ammesse unicamente se previste ai sensi del comma 1.

Per evitare fraintendimenti, il comma 4 fornisce, infine, la definizione dei termini comunicazione e diffusione utilizzati nel comma precedente, specificando che la comunicazione consiste nella trasmissione di dati o nella loro messa a disposizione a favore di destinatari che siano stati preventivamente individuati, mentre la diffusione consiste nel «dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione».

Tra comunicazione e diffusione esiste, dunque, una differenza sostanziale: la comunicazione è ammessa, qualora la stessa sia necessaria allo svolgimento delle finalità istituzionali, anche in assenza di previsione legislativa o regolamentare, previa comunicazione al Garante, che, però, può adottare «una diversa determinazione delle misure da adottarsi a garanzia degli interessati». La diffusione, invece, è ammessa esclusivamente se prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento.

L'art. 2-*sexies* detta le condizioni richieste per il "trattamento di categorie particolari di dati necessario per motivi di interesse pubblico rilevante". Il comma 1 – dopo aver richiamato l'art. 9, par. 1, GDPR, sul trattamento di categorie particolari di dati personali[20] – sfrutta il "margine di manovra" concesso agli Stati membri per regolare nello specifico i trattamenti delle "categorie particolari" in presenza di motivi d'interesse pubblico rilevante, ai sensi del par. 2, lett. *g*) del Regolamento. L'ammissibilità del trattamento presuppone che detti motivi siano previsti da una pluralità di fonti, sia dell'ordinamento dell'Unione europea, sia dell'ordinamento interno: disposizioni di legge o, nei casi previsti dalla legge, di regolamento. Il trattamento è ammissibile purché siano specificati, dalle fonti così individuate, «i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

La disposizione di legge o di regolamento, oltre ad assicurare le condizioni di

---

[19] Sulla questione della decorrenza dei quarantacinque giorni, cfr. S. D'ANCONA, *op. cit.*, p. 598.

[20] Come già affermato *supra*, «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

proporzionalità del trattamento, deve specificare, a salvaguardia del diritto alla protezione dei dati e delle misure di tutela per gli interessati, i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo d'interesse pubblico rilevante.

Il comma 2 elenca i trattamenti che possono essere effettuati per motivi di rilevante interesse pubblico.

Da segnalare l'accesso ai documenti amministrativi, in nome del fondamentale principio di trasparenza dell'azione amministrativa: l'attività di stato civile e di tenuta dei pubblici registri (bene della certezza pubblica); la documentazione istituzionale (a garanzia del principio di responsabilità politica e amministrativa); gli accertamenti tributari; le attività amministrative d'ispezione, di controllo e sanzionatorie. Compaiono anche qui i compiti di igiene, sicurezza e salute, già considerati dal GDPR, e le funzioni archivistiche e statistiche.

In forza del rinvio operato dal comma 3 dell'art. 2-*sexies* all'art. 2-*septies*, i dati genetici, biometrici e relativi alla salute possono essere oggetto di trattamento in presenza di una delle condizioni previste dall'art. 9, par. 2, del Regolamento e in conformità alle misure di garanzia disposte dal Garante.

L'art. 2-*quinquiesdecies* disciplina, infine, la potestà del Garante [21], ai sensi dell'art. 36, par. 5, del Regolamento. Per quanto riguarda i rapporti tra l'Autorità di controllo e coloro che trattano i dati personali nella Pubblica Amministrazione, il Regolamento dispone espressamente che i secondi devono cooperare con la prima ai sensi dell'art. 31 [22].

II Garante ha la possibilità, nel caso di trattamenti che, per l'esecuzione di un compito di interesse pubblico, presentino rischi elevati per gli interessati, di prescrivere, «con provvedimenti di carattere generale adottati d'ufficio», al titolare del trattamento «misure e accorgimenti a garanzia dell'interessato», che il titolare è tenuto ad adottare. La sfera dei poteri correttivi, a cui il Garante può fare ricorso, varia dal semplice avvertimento a interventi più incisivi [23].

5. *Comunicazione e diffusione dei dati: base giuridica*

Premesso che il concetto di trattamento dei dati personali racchiude tutte le operazioni che implicano la conoscenza di dati personali [24], il Regolamento stabi-

---

[21] Artt. 154 e 154-*bis*, Codice in materia di protezione dei dati personali, come modificato dal d.lgs. 10 agosto 2018, n. 101.

[22] «Il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il loro rappresentante cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti».

[23] L'art. 154-*ter* ("*Potere di agire e rappresentanza in giudizio*"), introdotto dall'art. 14, d.lgs. 10 agosto 2018, n. 101, conferisce al Garante la legittimazione «ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali».

[24] L'art. 4 del Regolamento definisce il trattamento dei dati personali «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a

lisce che il trattamento deve trovare fondamento in una base giuridica. Ciò determina per il titolare del trattamento[25] l'obbligo di individuare la base giuridica più idonea rispetto al trattamento che deve effettuare.

L'art. 6 (*Liceità del trattamento*) stabilisce la tipologia delle basi giuridiche e le condizioni secondo le quali il trattamento è lecito.

Il trattamento è lecito se ricorre una delle sei seguenti condizioni giuridiche:

«*a*) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità[26];

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

Per quanto riguarda la Pubblica Amministrazione è importante sottolineare che la lett. *f*) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Il trattamento necessario per l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di poteri pubblici, condizione prevista dalla lett. *e*), non richiede il consenso, né deve essere garantita la portabilità[27], ma richiede che sia

---

dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

[25] Regolamento, art. 4, definizioni: «7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

[26] Il consenso al trattamento dei dati personali non è definitivo; è previsto, infatti, il diritto della revocabilità del consenso prestato, che garantisce al richiedente interessato la cancellazione dei dati personali forniti in precedenza al titolare del trattamento: art. 7, punto 3, Regolamento. Sul consenso al trattamento dei dati personali, v. A. Pisapia, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, Torino, 2018, pp. 57-64.

[27] Art. 20 Regolamento. Sulla portabilità dei dati, v. M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorr. regole*, 2/2018, pp. 225-245.

fornita l'informativa sulla privacy, nella quale va indicata tassativamente la base giuridica del trattamento e specificata per legge la finalità.

Col GDPR si passa da una visione che richiedeva la prova di aver adempiuto determinate formalità, ad una prospettiva imperniata sul principio di *accountability*[28] o di responsabilizzazione: il titolare del trattamento dei dati è tenuto a mettere in atto tutte le misure necessarie perché il trattamento sia conforme ai principi del GDPR[29], ma anche a riesaminarle ed aggiornarle[30].

Il principio di *accountability* richiede, quindi, l'adozione di appropriate misure *ex ante*, nella fase di elaborazione e predisposizione dei processi, ma anche regolari verifiche *ex post* «per controllare la tenuta del sistema»[31]. Questo processo, denominato *Privacy Impact Assessment* (PIA), si fonda sulla necessità di valutare l'impatto del trattamento dei dati al fine di attivare misure di sicurezza adeguate. Mentre prima gli adempimenti erano basati su criteri formali e sulla logica dell'effettivo abuso dei dati raccolti, ora diventa obbligatorio «un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al regolamento»[32]. Il titolare del trat-

---

[28] Il principio di *accountability*, di derivazione anglosassone, rappresenta uno dei pilastri su cui si fonda l'impianto normativo del Regolamento ed è previsto dagli artt. 5, par. 2, e 24 del Regolamento stesso: «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento». Per un approfondimento, G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in ID., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., pp. 14-16; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, I, *Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli,Torino, 2016, pp. 279-286; ID., *Privacy e il diritto europeo alla protezione dei dati personali*, II, *Il Regolamento europeo 2016/679*, Giappichelli, Torino, 2016; A. PISAPIA, *op. cit.*, pp. 99-101; G. RUSSO e M. POLINI, *I principi di accountability e di effettività nel nuovo regolamento*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali. La privacy dopo il regolamento UE 2016/679*, Maggioli Editore, Santarcangelo di Romagna, pp. 127-132.

[29] Sul trattamento dei dati personali v. anche il Considerando 146: «Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento».

[30] «Il titolare è il centro di imputazione delle decisioni sulle finalità e sui mezzi del trattamento»: E. PELINO, *I soggetti del trattamento*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 121.

[31] A. PISAPIA, *op. cit.*, p.101. V., anche, C. BISTOLFI, *Le obbligazioni di compliance in materia di protezione dei dati*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, *op. cit.*, p. 323.

[32] M. MAGLIO, *Il regolamento europeo 2016/679 in materia di dati personali: inquadramento generale e prospettive di sviluppo*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali*, cit., pp. 62-63. L'art. 30 del Regolamento impone, a proposito del sistema documentale, al titolare del trattamento la tenuta di un registro (art. 30 e Considerando 171), redatto in forma scritta o elettronica, delle attività svolte sotto la sua responsabilità,

tamento deve provare di aver adottato misure adeguate ed efficaci[33].

Il principio di responsabilizzazione fa sì che possano essere individuate, in caso di non conformità del trattamento dati rispetto alla normativa, responsabilità amministrative, elencate all'art. 166, commi 1 e 2, civili per risarcimento per fatto illecito, *ex* art. 2043 cod. civ.[34], per responsabilità per l'esercizio di attività pericolose, *ex* art. 2050 cod. civ., per responsabilità solidale, *ex* art. 2055 cod. civ. e, infine, penali a carico del titolare del trattamento e del responsabile del trattamento[35], ma anche di chiunque tratti illecitamente i dati, ai sensi degli artt.167, 167-*bis*, 167-*ter* e 168[36] del d.lgs. 30 giugno 2003, n. 196, in modo tale da far rispettare i principi generali del trattamento dei dati personali[37].

Il titolare del trattamento, per espletare al meglio i suoi compiti, deve impegnarsi a proteggere i dati con cui entra in contatto adottando misure tecniche e organizzative adeguate, quali la pseudonimizzazione[38] e la minimizzazione[39], e a

---

che deve essere messo a disposizione del Garante nel caso in cui lo richieda. In questo modo sarà possibile al titolare «dimostrare quali misure tecniche ed organizzative ha utilizzato per garantire un livello di sicurezza adeguato al rischio e soprattutto che tali misure sono state messe in atto»: G. Russo e M. Polini, *op. cit.*, p. 133.

[33] Art. 5, par. 2, Regolamento. Cfr. C. Bistolfi, *Le obbligazioni di compliance in materia di protezione dei dati*, cit., pp. 325-327.

[34] F. Di Resta, *op. cit.*

[35] Il titolare ed il responsabile rispondono per il danno cagionato all'interessato nel caso in cui il trattamento violi quanto disposto dal Regolamento, inoltre, il responsabile del trattamento ne risponde nel caso in cui abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare. La ripartizione della responsabilità civile e dell'onere della prova nel rapporto tra titolare e responsabile si basa sul contenuto della nomina e/o del contratto di servizio. La norma individua anche le condizioni per cui il titolare o il responsabile del trattamento sono esonerati da responsabilità: l'uno e/o l'altro devono dimostrare che l'evento dannoso non è loro imputabile e di avere adottato tutte le misure idonee ad evitare il danno. Vi è, quindi, un'inversione dell'onere della prova a carico del titolare e del responsabile del trattamento dei dati.

[36] Artt. 24-27 Regolamento. Con il d.lgs. 10 agosto 2018, n. 101, è stata riformata, inasprendo le sanzioni, buona parte della disciplina previgente per regolamentare la responsabilità amministrativa, civile e penale in ambito di trattamento di dati personali.

[37] Il Regolamento all'art. 5, par. 1, pone i seguenti principi: liceità, correttezza e trasparenza del trattamento; raccolta per finalità determinate, esplicite e legittime, e successivo trattamento non incompatibile con tali finalità; minimizzazione dei dati; esattezza e aggiornamento; conservazione dei dati per il solo tempo necessario al conseguimento delle finalità per le quali sono trattati; integrità e riservatezza.

[38] La pseudonimizzazione richiede che, nelle banche dati, i dati personali siano scollegati dalle identità delle persone. Tale "pratica", che non preclude ulteriori misure di protezione dei dati, per il Considerando 28 GDPR, «può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati».

[39] La minimizzazione riassume i principi di adeguatezza, pertinenza e limitazione rispetto alla finalità per cui i dati sono trattati; «l'applicazione dei tre principi ha l'obiettivo di rendere la raccolta di dati quanto più specifica possibile, minimizzando la quantità di dati acquisiti e

integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti previsti dal GDPR e tutelare i diritti degli interessati [40], sempre nel rispetto del principio di proporzionalità.

Il titolare del trattamento, per espletare i suoi compiti, si può avvalere dal punto di vista operativo del responsabile del trattamento, ai sensi dell'art. 28 del Regolamento, che prevede la possibilità di nomina di un soggetto con compiti definiti da parte del titolare per la gestione del trattamento dei dati personali. In definitiva, il titolare, con un contratto, in quanto l'atto di designazione deve essere vincolante, delega al responsabile la concreta gestione del trattamento [41].

Pur nella differenza dei ruoli, il titolare e il responsabile del trattamento rivestono una funzione comune: entrambi, sia pure a titolo diverso, hanno la responsabilità giuridica del rispetto degli obblighi imposti dalla normativa. Chi assume l'uno e l'altro di questi due ruoli risponde, per la parte del trattamento che gli compete, delle eventuali violazioni della normativa [42].

Per la protezione dei dati è prevista anche una terza nuova figura, estremamente importante, il *Data Protection Officer* [43] (DPO) o Responsabile Protezione Dati (RPD), che deve essere designato dal titolare del trattamento e dal responsabile del trattamento dei dati personali in numerosi casi e, specificamente, nel caso in cui il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali [44]; è prevista qualche eccezione (ad esempio, i piccoli comuni possono condividerlo) [45].

È opportuna un'ulteriore precisazione sul principio di responsabilizzazione.

---

limitando la collezione ai soli dati necessari per il perseguimento delle finalità predeterminate»: L. Bolognini, *Pertinenza, adeguatezza, non eccedenza rispetto alle finalità*, in L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy*, cit., p. 107.

[40] Art. 25, par. 1, Regolamento.

[41] Il contratto di nomina deve contenere le seguenti indicazioni: le categorie di dati personali da trattare, i trattamenti delegati al responsabile, le finalità ed i mezzi del trattamento, le misure di sicurezza da adottare, precise istruzioni su come adempiere all'incarico ricevuto e la sua durata. Il responsabile del trattamento può, a sua volta, nominare dei sub–responsabili, a meno che ciò non gli sia vietato dalle istruzioni del titolare del trattamento, ma deve rispondere del loro operato al titolare del trattamento.

[42] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, I, cit., p. 198.

[43] Sull'importanza di tale figura, cfr. il parere del Gruppo dei Garanti europei *ex* art. 29, del 13 dicembre 2016. Il Gruppo di lavoro *ex* art. 29, istituito dall'art. 29 della direttiva 95/46, era composto dai rappresentanti delle Autorità di protezione dati personali di ciascun Stato membro. Come si è anticipato, con l'entrata in vigore del *General Data Protection Regulation* il 28 maggio 2018, il Gruppo è stato sostituito dal Comitato europeo per la protezione dei dati.

[44] Art. 7, lett. *a*), Regolamento.

[45] Al DPO, che è una nuova figura introdotta dal Regolamento (artt. 37– 39), la cui nomina è obbligatoria nella P.A., è richiesto di essere un esperto della normativa in tema di dati personali, considerati i suoi compiti di consulenza e di sorveglianza sul rispetto del GDPR e di ricognizione al fine anche di redigere il Registro delle attività di trattamento.

Ai titolari del trattamento è attribuito il compito di valutare in maniera autonoma i vari tipi di trattamento che intendono operare e di individuare e documentarne la base giuridica. Due importanti corollari di tale "operazione" sono la *privacy by design* e la *privacy by default*[46].

La *privacy by design* implica che la protezione dei dati debba essere integrata nel sistema di raccolta dei dati in modo da assicurare una tutela adeguata dei dati personali degli interessati e la valutazione e la previsione dei possibili rischi dovuti al trattamento dei dati stessi.

La *privacy by default* riguarda l'organizzazione della raccolta dei dati attraverso una modalità in grado di limitare all'indispensabile la raccolta dei dati stessi, predeterminando modalità del trattamento che richiedano una conservazione predefinita ed adeguata e tale da avvenire nella misura meno rischiosa e incisiva possibile, tanto dal punto di vista contenutistico quanto da quello temporale.

In virtù dei principi di *privacy by design* e di *privacy by default*, ogni procedimento della P.A., che implica un trattamento dei dati personali, deve tener conto del c.d. *risk based approach* e prendere, quindi, in considerazione fin dall'inizio le possibili implicazioni negative sulla privacy dei soggetti del trattamento.

Non solo: per rispettare la tutela dell'equilibrio delle parti interessate dal trattamento dei dati personali, anche l'impostazione di base dei dispositivi elettronici utilizzati dal titolare del trattamento deve essere effettuata nel senso più favorevole per la parte debole; la pubblica amministrazione è poi obbligata ad effettuare con *test* la valutazione dell'impatto del trattamento sulla privacy degli individui mediante una consultazione preventiva con il Garante della privacy.

Per il principio della responsabilizzazione o «rendicontazione», il titolare del trattamento e il responsabile del trattamento sono tenuti a rispondere in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dei danni materiali e immateriali dovuti alla violazione di quanto previsto dal GDPR[47]. Il regime di responsabilità nei confronti del titolare del trattamento si attua, come già detto, in sede civile sotto forma di tutela risarcitoria esperibile da chiunque abbia subito un danno materiale o immateriale dalla violazione delle norme del Regolamento a causa di inadempienze agli obblighi previsti dallo stesso. Tale diritto sorge nel momento in cui è posta in essere una condotta, attiva o omissiva, a danno del titolare dei dati trattati. In caso di pluralità di soggetti titolari del trattamento si applica l'art. 2055 del codice civile, mentre in sede penale sono appli-

---

[46] I principi della *privacy by design* e della *privacy by default* sono trattati all'art. 25, commi 1 e 2, GDPR; si vedano anche i Considerando 24-29, che definiscono le tecniche e le misure da attuare per garantire il loro rispetto. Ulteriori indicazioni si ricavano dalle linee guida dedicate al principio della trasparenza: *Article 29 Data Protection Working Party*, *Guidelines on trasparency under Regulation 2016/679, WP260*, 29 novembre 2017; cfr., sul punto, D. MESSINA, *Il Regolamento (UE) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analitica"*, in *Federalismi*, n. 20/2018, p. 17.

[47] Art. 82, parr. 2 e 4, Regolamento.

cabili le disposizioni penali del Codice per la protezione dei dati personali, alle quali sono state aggiunte le seguenti fattispecie: la violazione dei dati personali (*data breach*)[48], ossia l'acquisizione "fraudolenta" di essi, e la cessione a terzi di rilevanti quantità di dati personali[49].

6. *Circolazione dei dati e pubblici poteri nella* digital society

Un cenno meritano le questioni, di sicura rilevanza ai fini degli interessi pubblici in gioco, relative alla protezione dei dati degli individui, utenti e consumatori nella *digital society*[50].

Il ruolo crescente dei *Big Data* rappresenta, secondo un *report* Agcom, una tendenza irreversibile: per la stragrande maggioranza degli individui, una parte rilevante della vita privata, oltre che di quella lavorativa, si è trasferita in rete, diventando una delle principali sorgenti di dati[51].

---

[48] In caso di violazione dei dati personali c'è l'obbligo, ai sensi degli artt. 33 e 34, Regolamento, della c.d. *data breach notification*, non prevista nella direttiva 95/46/CE: il Titolare del trattamento deve comunicare eventuali violazioni dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza all'Autorità nazionale di protezione dei dati (art. 33) e all'interessato se la violazione dei dati rappresenta «un rischio elevato per i diritti e le libertà delle persone fisiche» (art. 34). Il titolare del trattamento deve comunicare all'interessato «con un linguaggio semplice e chiaro la natura della violazione dei dati personali» ed offrire indicazioni sulle misure adottate o che intende adottare per porre rimedio o limitare le possibili conseguenze negative della violazione. La comunicazione all'interessato non è richiesta se è stata soddisfatta una delle tre condizioni elencate al punto 3 dell'art. 34.

[49] Significativi, a questo proposito, sono il caso della acquisizione *Facebook/Whatsapp* e, soprattutto, la vicenda *Facebook-Cambridge Analytica*, sorta nel marzo 2018, quando *The Observer*, *The Guardian* e *The New York Times* rivelarono che *Cambridge Analytica*, azienda di consulenze e *marketing online*, specializzata nella profilazione degli utenti dei *social network*, attraverso le tracce lasciate da essi durante la navigazione *online*, aveva raggiunto, utilizzando i dati degli utenti di *Facebook* che le erano stati ceduti dal *social network* di *Palo Alto*, milioni di elettori statunitensi, con messaggi mirati durante la campagna presidenziale negli USA del 2016.

[50] I.S. Rubinstein, *Big Data: The End of Privacy or a New Beginning*?, in *International Data Privacy Law*, 3, 2013, pp. 74-87.

[51] AGCOM, Servizio economico-statistico, *Big data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*. I *Big Data* sono «*information assets* caratterizzati da un volume, da una velocità e da una varietà tali da richiedere l'utilizzo di tecnologie e metodi di analisi specifici per estrarne valore»: A. De Mauro, M. Greco, M. Grimaldi, *A Formal definition of Big Data based on its essential Features*, in *Library Review*, vol. 65, n. 3, 2016, pp. 122-135. Sull'impatto dei *Big Data* nella tutela dei dati personali, v. Consiglio d'Europa, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasburgo, 2017. D. Laney, in uno studio del 2001 (*3D Data Management: Controlling Data Volume, Velocity, and Variety*, reperibile in *http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-*

I *Big Data*, in una prima accezione[52], sono quei dati che l'utente immette all'interno delle piattaforme *online* per poter usufruire dei servizi e dei beni offerti e che transitano attraverso *Internet*, formando quella che è stata definita *datasphere*. In una seconda accezione, il termine è utilizzato in riferimento alla capacità di analizzare una massa di dati eterogenei, strutturati e non strutturati, attraverso sofisticati algoritmi per i più diversi fini.

Numerosi e rilevanti sono gli interessi pubblici che hanno spinto le istituzioni politiche, europee e statali e, soprattutto, le Autorità indipendenti ad approfondire tale tematica[53]: i *Big Data* hanno un considerevole valore economico (i dati sono il "petrolio" dell'economia digitale), possono essere immagazzinati in maniera non le-

---

Velocity-and-Variety.pdf) definì il modello di crescita dei *Big Data* come caratterizzato da "3V", correlate tra loro: il modello è determinato dal costante aumento, nel tempo, del Volume, della *velocità* e della *varietà* dei dati. La gestione combinata delle "3V" ha richiesto nuove tecniche di analisi per generare valore dai *Big Data* e trovare opportunità commerciali attraverso la profilazione degli individui operanti su *Internet*. Il modello delle "3V" in seguito è stato modificato e ampliato, nel 2017 erano già state individuate "42 V": T. SHAFER (2017), *"The 42 V's of Big data and Data Science", Elder Research-Data Science & Predictive Analytics*, *https://www.elderresearch.com/company/blog/42-v-of-big-data*. Di queste "42 V", le più importanti, oltre alle prime "3V", sopra richiamate, sono quelle di veridicità, valore, valenza e visualizzazione.

[52] Si parla di *Big Data* quando si ha una mole di dati nell'ordine degli *zettabyte*, ovvero miliardi di *terabyte*, per averne un'idea approssimativa si può ricordare che un «*zettabyte* corrisponde a una capacità di archiviazione pari a oltre 36.000 anni (in termini di durata) di video in HD ovvero una pila composta da 250 miliardi di DVD»: AGCOM, *Big data. Interim report*, cit. Il *report* riprende, in particolare, un articolo apparso sul *Guardian*, *Goodbye petabytes, hello zettabytes*, *https://www.theguardian.com/technology/2010/may/03/humanity-digital-output-zettabyte*, 2010 e altri due contributi: *From Bits to Brontobytes, The Oxford Math Center, http://www.oxfordmathcenter.com/drupal7/node/410* e *The Zettabyte Era: Trends and Analysis, CISCO Public white paper*, *June*, 2017.

[53] Una delle preoccupazioni al centro dell'attenzione generale riguarda la tutela della privacy in quanto le tecniche di *data mining*, attraverso l'elaborazione delle informazioni immagazzinate, anche se anonime, violano la riservatezza dei dati personali e sono in grado di individuare gli individui reali, dal momento che grazie all'utilizzo dei *Big Data* attraverso incroci di *database* o tecniche di re-identificazione è possibile ricondurre informazioni anche anonime ad un singolo individuo reale. A testimonianza della trasversalità del tema, in data 30 maggio 2017, è stata avviata un'indagine conoscitiva congiunta che coinvolge l'Autorità Garante della Concorrenza e del Mercato (AGCM), il Garante per la protezione dei dati personali e l'Autorità per le Garanzie nelle Comunicazioni (AGCOM), finalizzata all'individuazione di eventuali criticità concorrenziali connesse ai *Big Data* e alla definizione di un quadro di regole atto a promuovere e tutelare la concorrenza dei mercati dell'economia digitale, consentendo al contempo una più efficace realizzazione dei compiti istituzionali di ciascuna Autorità. Finocchiaro, opportunamente, richiama l'attenzione prestata al tema della tutela della privacy dalla recente giurisprudenza della Corte del Lussemburgo: G. FINOCCHIARO, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir.inf.*, 2015, p. 281. Sul caso *Schrems*, riguardante l'efficacia transazionale delle tutele, v. G. GIANNONE CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Dir. inf.*, 2015, pp. 271 ss.

gale e utilizzati per "catalogare" gli utenti del *web* in vista del *microtargeting* comportamentale (messaggi pubblicitari specializzati sulla singola persona)[54]. La potenziale lesione della sfera della persona va di pari passo con il *vulnus* alla dinamica concorrenziale provocato dalle nuove forme di abuso della posizione di dominanza economica[55].

Sorgono questioni che potranno richiedere ulteriori interventi normativi a livello sovranazionale: il dilemma che si pone alle istituzioni politiche è come garantire i diritti delle persone e il patrimonio dei loro dati[56], senza, però, bloccare la spinta imponente che alla crescita economica viene dalla circolazione dei dati stessi. È il dilemma cui il Regolamento europeo dà una prima e articolata risposta, che ha suscitato attenzione anche sull'altra sponda dell'Atlantico, testimoniando la forza attrattiva della normativa europea[57].

---

[54] «Quella che nella televisione tradizionale era una campagna pubblicitaria indifferenziata, che raggiungeva consumatori più o meno interessati al prodotto, può diventare, nel mondo di *Internet*, una campagna selettiva, che raggiunge e si adatta ai gusti dei diversi utenti, differenziando messaggi e proposte a seconda dei singoli utenti. Con un valore molto maggiore per gli inserzionisti e introiti pubblicitari più elevati per le piattaforme»: M. POLO, *La concorrenza al tempo dei big data*, in *lavoce.info*, 26 gennaio 2018. Grazie ai *Big Data*, le imprese selezionano i consumatori, pongono indagini di tipo mirato sugli stessi e offrono prodotti che si basano sulle loro preferenze. Per A. AKERLOV e R. SHILLER, *Phishing for Phools: The Economics of Manipulation and Deception*, *Princeton University Press*, 2015, l'inganno e la manipolazione non sono fenomeni economici marginali, ma sono alla base di un assetto di mercato in cui i consumatori sono continuamente soggetti al *Phishing for Phools*, attività tesa a sfruttarne le debolezze a livello psicologico e informativo, inducendoli spesso a prendere decisioni che vanno contro il loro interesse. Per una critica più ampia, C. O'NEILL, *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia*, Bompiani, Milano, 2018.

[55] È osservazione diffusa che le grandi imprese operanti nella *digital society*, come *Google*, *Facebook*, *Apple*, *Amazon*, potendo fare affidamento su una quantità crescente di dati immagazzinati, sono in grado di offrire un servizio sempre più efficiente, che permette loro di acquisire un potere in grado di dar vita per gli utenti ad effetti di *lock-in* (vincoli anticoncorrenziali), di rendere estremamente difficile l'operatività delle piccole e medie aziende operanti nello stesso settore e di impedire la nascita di nuove imprese. Sulle fusioni guidate da strategie collegate al possesso dei *Big Data*, cfr. A. BUTTÀ, *Conglomerate effects in the digital ecosystem: network effects, privacy and big data in the Microsoft/Linkedin merger*, in *Concorrenza e Mercato*, vol. 24/2017, pp. 449-450, 455-456. Tra i molteplici casi riguardanti le fusioni tra aziende operanti attraverso *Internet*, v. il *case M. 8228 – Facebook/Whatsapp* (*Commission decision of 17. 5. 2017 imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for the supply by an undertaking of incorrect or misleading information*).

[56] Particolarmente importanti per la profilazione sono le tracce lasciate dai *device* mobili, dal momento che essi, essendo personali, sono utilizzati solitamente da un solo individuo.

[57] Si è osservato, commentando i casi *Google Spain* (CGUE, Grande sez., 13 maggio 2014, causa C-131/12, *Google Spain, Google Inc. c. AEPD, Costeja Gonzáles*) e *Schrems* (CGUE, Grande sez., 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*), l'anno precedente all'emanazione del Regolamento UE, che la Corte di giustizia europea si è fatta «promotrice del modello europeo del diritto alla protezione dei dati personali», affermando

Il rilievo di tali temi per la tutela della persona è tale da giustificare l'auspicio di convergenze e concertazioni tra sistemi giuridici di diversa ispirazione e tradizione.

«l'applicabilità della normativa europea anche nel caso in cui i titolari di trattamento dei dati personali siano soggetti non europei e i dati vengano trattati prevalentemente fuori dall'Europa»: G. FINOCCHIARO, *La giurisprudenza della Corte di giustizia*, cit., pp. 279-280. Sul caso *Google Spain* v. E. KELSEY, *Case Analysis – Google Spain SL and Google Inc. v AEPD and Mario, Costeja Gonzáles: Protection of personal data, freedom of information and the "right to be forgotten"*, in *European Human Rights Law Review*, 2014, pp. 395 ss.