La disciplina dei diversi rapporti che riguardano i dati personali

Chiara Angiolini, Elia Cremona[1]

Abstract: This chapter highlights the variety of relationships involving personal data. The first paragraphs focus on relations between parties other than data subjects, such as contractual relationships between data controllers and between data controller and data processor. The following paragraphs deal with the relationships between public bodies and private actors with regard to the use of data, and between data intermediaries and actors who seek access to data. Finally, in the last paragraph, Data Act rules are analysed specifically in relation to the new access rights on IoT data.

Keywords: Data protection agreements, data transfer agreements, open data, data altruism, data intermediation services, access rights on IoT data

1. La varietà dei rapporti che riguardano i dati personali

Nei precedenti capitoli si è detto dei diversi ruoli esistenti in relazione al trattamento, in particolare quelli di titolare del trattamento e di responsabile del trattamento (v. cap. *Le definizioni fondamentali*).

In questo capitolo si prendono in esame le regole relative ai rapporti fra tali soggetti, guardando sia agli atti che devono essere adottati ai sensi del Reg. UE 2016/679 (d'ora in avanti: GDPR), anche con riguardo ai trasferimenti verso paesi terzi e organizzazioni internazionali, sia al ruolo del contratto rispetto ai trattamenti che consistono nella comunicazione e nella ricezione dei dati personali fra titolari del trattamento.

[1] Chiara Angiolini ha scritto i paragraafi 1, 2, 3, 4, 5, 7.2 e 8; Elia Cremona ha scritto i paragrafi 6, 7 e 7.1.

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it
Elia Cremona, University of Siena, Italy, elia.cremona@unisi.it, 0000-0001-9336-218X

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Inoltre, occorre evidenziare come, negli ultimi tempi, i dati personali siano divenuti oggetto di una regolamentazione di rapporti soggettivi che trovano disciplina al di fuori del GDPR. Con l'intento di far circolare maggiormente i dati detenuti da soggetti pubblici e privati, la direttiva UE 2019/1024 (d'ora in avanti: Direttiva *Open Data*), il regolamento UE 2022/868 (d'ora in avanti: *Data Governance Act*) e il regolamento UE 2023/2854 (d'ora in avanti: *Data Act*) hanno messo i dati, personali e non, al centro di una serie di relazioni disciplinate attraverso varie qualificazioni soggettive e complesse regole volte anche alla valorizzazione dei dati nei più ampi contesti sociali.

In questo capitolo, si prendono dunque in esame anche le regole relative a questi ulteriori rapporti riguardanti i dati personali.

2. I contratti fra contitolari del trattamento

In ogni caso di contitolarità del trattamento, ai sensi dell'art. 26 GDPR i contitolari devono determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR (sull'informazione all'interessato, v. cap. *I diritti dell'interessato*), salvo il caso in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

L'accordo può designare un punto di contatto per gli interessati e deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo deve essere messo a disposizione dell'interessato.

L'art. 26 GDPR dispone anche che, indipendentemente da quanto prevede l'accordo fra contitolari, l'interessato possa esercitare i propri diritti ai sensi del GDPR nei confronti di e contro ciascun titolare del trattamento.

Rispetto a tale accordo, come già detto nel capitolo 3, è di particolare importanza la sentenza della Corte di Giustizia dell'UE del 4 maggio 2023 C- 60/22, secondo cui non si è di fronte ad un trattamento illecito quando vi è la violazione delle regole in merito agli accordi di contitolarità, poste dall'art. 26 GDPR. La Corte poggia tale conclusione su vari argomenti, fra cui quello secondo cui

> l'assenza di un accordo che determini la contitolarità, ai sensi dell'articolo 26 del RGPD […] non è sufficiente a dimostrare, di per sé, l'esistenza di una lesione del diritto fondamentale alla protezione dei dati personali. In particolare, se è vero che […] la chiara ripartizione delle responsabilità tra i contitolari del trattamento e il registro delle attività di trattamento costituiscono mezzi per garantire il rispetto, da parte di tali contitolari, delle garanzie previste da detto regolamento per la tutela dei diritti e delle libertà degli interessati, resta nondimeno il fatto che l'assenza di un siffatto registro o di un siffatto accordo non dimostra, di per sé, che tali diritti e tali libertà siano stati violati. (*Ibidem*, § 65)

3. L'atto fra il titolare e il responsabile del trattamento

L'art. 28 GDPR, rubricato «Responsabile del trattamento» prevede che i trattamenti da parte di un responsabile del trattamento siano disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.

Tale atto deve vincolare il responsabile del trattamento al titolare del trattamento e deve regolare la materia che ne è l'oggetto e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

In particolare, il contratto o altro atto giuridico deve prevedere che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 GDPR;

d) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III GDPR;

e) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 GDPR in materia di sicurezza del trattamento, violazione dei dati personali (*data breach*), valutazione di impatto, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

f) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

g) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Il responsabile del trattamento deve informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Inoltre, nell'atto di cui all'art. 28 GDPR si deve prevedere che siano rispettate le regole poste dal medesimo articolo relative alla nomina dei c.d. sub-responsabili del trattamento, che si illustrano di seguito.

In primo luogo, l'art. 28 GDPR prevede che il responsabile del trattamento non ricorra a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento deve informare il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Inoltre, quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Infine, qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

L'art. 28 GDPR prevede anche che il contratto o altro atto giuridico di nomina del responsabile possano basarsi su clausole tipo stabilite dalla Commissione Europea. La Commissione Europea ha adottato tali clausole con la Decisione di Esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, GDPR e dell'articolo 29, paragrafo 7, del Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio.

4. I contratti fra titolari del trattamento per la comunicazione dei dati personali, nella prospettiva del diritto privato

Ad di là di atti e accordi che siano obbligatori ai sensi del GDPR, di cui si è detto nei precedenti paragrafi, è utile dare un quadro delle questioni che concernono i contratti relativi la comunicazione di dati personali fra titolari del trattamento dal punto di vista del diritto privato.

L'inquadramento di tali contratti non è semplice.

Si può cominciare richiamando la nozione di titolare del trattamento, secondo cui si diventa titolari del trattamento quando si determinano le finalità e i mezzi del trattamento (v. cap. *Le definizioni fondamentali*, § 3.5). Proprio in ragione di tale definizione basata sul ruolo di un soggetto rispetto al trattamento, non è possibile trasferire la qualifica di titolare del trattamento.

Dunque, non è corretto discorrere di trasferimento della posizione di titolare del trattamento, ed è invece utile concentrarsi sulla facoltà di una parte di comunicare o diffondere i dati personali, e di quella dell'altro contraente di riceverli, e dunque di raccoglierli.

Entrambe le attività sono da considerare come trattamenti di dati personali, sottoposti al requisito della liceità (sulla liceità del trattamento, v. cap. *La disciplina dell'attività di trattamento*).

Allora, quando il titolare abbia la facoltà di comunicare i dati a un terzo, e questi possa raccoglierli in ragione di una base giuridica del trattamento (v. cap. *La disciplina dell'attività di trattamento*), le parti possono regolare tale comunicazione tramite un contratto, anche verso un corrispettivo. In questi casi il contratto rende possibile l'accesso ai dati personali da parte di un nuovo titolare del trattamento, obbligando il titolare originario a comunicarglieli, ma non trasferisce una situazione giuridica soggettiva fra le due parti, in quanto il nuovo titolare del trattamento potrà trattare i dati in ragione delle basi giuridiche che può far valere e che ha scelto e di cui ha informato l'interessato (sull'informazione dell'interessato v. cap. *I diritti dell'interessato*).

Occorre ora considerare l'ipotesi in cui la comunicazione dei dati da parte del primo titolare sia illecita ai sensi del GDPR e quella in cui lo sia la raccolta da parte del titolare destinatario dei dati (Angiolini, 2020).

Quando la comunicazione non sia lecita da parte del primo titolare del trattamento, il contratto deve essere considerato nullo per illiceità dell'oggetto *ex* art 1418, secondo comma c.c. Infatti, in questo caso è la prestazione stessa ad essere illecita, e dunque l'oggetto del contratto sarà da considerarsi carente del requisito della liceità, posto dall'art. 1346 c.c.

Ove invece la comunicazione dei dati personali da parte del primo titolare è lecita, e ad essere illecita è la raccolta da parte del destinatario della comunicazione, il contratto sarà da ritenersi nullo *ex* art 1418, 2 comma, c.c., in quanto ne sarà illecita la causa, in relazione alla funzione concreta che questo realizza di permettere al secondo titolare di avere accesso ai dati personali – e dunque *in primis* di raccoglierli.

Nelle due ipotesi che si sono viste in cui il contratto è nullo, l'interessato potrà far valere la nullità del contratto. Questo in quanto nell'applicare l'art. 1421 c.c. in tema di legittimazione a far valere la nullità, è da considerare che l'interessato è titolare di diritti sui dati personali che sono oggetto di comunicazione, e dunque parte che può dirsi senz'altro essere pregiudicata da un trattamento illecito. Tale ipotesi è comunque al momento più che altro di scuola, considerando l'elevato grado di opacità di tali rapporti contrattuali.

5. I flussi transfrontalieri di dati personali

Il capo V del GDPR è dedicato ai trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali e prevede una disciplina articolata, che è stata oggetto di vari interventi della Corte di Giustizia dell'UE.

L'art. 44 GDPR, rubricato «principio generale per il trasferimento» è di particolare importanza e recita:

> Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati

> personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Gli articoli successivi del GDPR prevedono diversi strumenti relativi al trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali, che sono i seguenti:

i) Trasferimento sulla base di una decisione di adeguatezza (art. 45);
ii) Trasferimento soggetto a garanzie adeguate (artt. 46-47);
iii) Deroghe in specifiche situazioni (art. 49).

5.1. Il trasferimento sulla base di una decisione di adeguatezza

In base a quanto dispone l'art 45 GDPR la Commissione Europea può decidere che un paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. In tal caso il trasferimento può essere compiuto, naturalmente nel rispetto del GDPR e della disciplina applicabile.

L'art. 45 GDPR individua gli elementi che la Commissione deve prendere in considerazione, in particolare, per valutare l'adeguatezza del livello di protezione, che sono i seguenti:

a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e la possibilità di un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;

b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e

c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

Dal punto di vista procedurale, la Commissione decide mediante atti di esecuzione. L'atto di esecuzione deve prevedere un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale.

Inoltre, la Commissione deve controllare su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni di adeguatezza adottate.

Se risulta dalle informazioni disponibili, in particolare in seguito al riesame periodico di cui si è appena detto, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di adeguatezza, mediante atti di esecuzione senza effetto retroattivo.

La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato. Nel momento in cui si scrive, giugno 2025, la Commissione ha adottato decisioni di adeguatezza relative a vari paesi, fra cui l'Argentina, il Regno Unito, Stati Uniti, Svizzera, Giappone.

Rispetto alla valutazione di adeguatezza è di particolare interesse la sentenza della Corte di Giustizia 16 luglio 2020 C-311/18, in cui la Corte ha giudicato invalida la decisione di adeguatezza relativa ai trasferimenti verso gli Stati Uniti (decisione di esecuzione UE 2016/1250 della Commissione, del 12 luglio 2016, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy). La pronuncia è di particolare rilevanza perché affronta alcuni aspetti importanti relativi all'interpretazione dell'art. 45 GDPR.

In particolare, la Corte, interpretando la disciplina del GDPR alla luce della Carta dei Diritti Fondamentali dell'UE ha statuito che:

i) l'adozione, da parte della Commissione, di una decisione di adeguatezza ai sensi dell'art. 45 GDPR richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell' ordinamento giuridico dell'Unione, interpretato alla luce dei diritti fondamentali protetti dalla Carta dei Diritti Fondamentali dell'UE, e in particolare gli artt. 7 (Rispetto della vita privata e della vita familiare, su cui si veda il cap. *Le fonti della disciplina in materia di dati personali*), 8 (Diritto alla protezione dei dati personali, su cui si veda il cap. *Le fonti della disciplina in materia di dati personali*) e 47 CDFUE (diritto a un ricorso effettivo e a un giudice imparziale);

ii) nel valutare l'adeguatezza del livello di protezione garantito da un paese terzo, la Commissione deve prendere in considerazione in particolare i mezzi di «ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento», anche alla luce dell'art. 47 CDFUE, che sancisce il diritto a un ricorso effettivo e a un giudice imparziale.

5.2. *Segue*. Il trasferimento soggetto a garanzie adeguate

Secondo quanto prevede l'art. 46 GDPR, In mancanza di una decisione di adeguatezza *ex* art. 45 GDPR, di cui si è appena detto, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se:

i) ha fornito garanzie adeguate e

ii) a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Con riguardo alle garanzie adeguate, occorre distinguere le ipotesi che necessitano di un'autorizzazione specifica da parte dell'autorità di controllo e quelle che non la necessitano.

Fatta salva l'autorizzazione dell'autorità di controllo competente, possono costituire garanzie adeguate:

a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o

b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati. L'autorità di controllo in questi casi applica il meccanismo di coerenza di cui all'articolo 63 (v. cap. *La regolamentazione e la tutela amministrativa*).

Inoltre, possono costituire garanzie adeguate, senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;

b) le norme vincolanti d'impresa in conformità dell'articolo 47 GDPR;

c) le clausole tipo di protezione dei dati adottate dalla Commissione;

d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione;

e) un codice di condotta approvato a norma dell'articolo 40 GDPR, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati;

f) un meccanismo di certificazione approvato a norma dell'articolo 42 GDPR, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Con riguardo alle clausole tipo di protezione dei dati adottate dalla Commissione, queste sono state adottate dalla Commissione con la decisione di esecuzione (UE) 2021/914 del 4 giugno 2021.

Per quanto riguarda le norme vincolanti per l'impresa, la procedura per la loro approvazione è prevista dall'art. 47 GDPR. In particolare, l'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63 GDPR (v. cap. *La regolamentazione e la tutela amministrativa*), a condizione che queste a norma dell'art. 47 GDPR:

1) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;

2) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;

3) specifichino almeno:

a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;

b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;

c) la loro natura giuridicamente vincolante, a livello sia interno che esterno;

d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;

e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22 GDPR, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79 GDPR, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;

f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;

g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14 GDPR (su tali informazioni v. cap. *I diritti dell'interessato*);

h) i compiti del responsabile della protezione dei dati (v. cap. *Le definizioni fondamentali*) o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami;

i) le procedure di reclamo;

j) meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;

k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;

l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);

m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa;

n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa.

Ancora con riguardo alle norme vincolanti per l'impresa, si possono poi citare, e assumono particolare rilevanza anche dal punto di vista operativo, le Raccomandazioni 1/2022 dell'EDPB sulla domanda di approvazione e sugli elementi e sui principi che devono figurare nelle norme vincolanti d'impresa del titolare del trattamento (articolo 47 del GDPR), adottate il 20 giugno 2023.

Rispetto ai trasferimenti soggetti a garanzie adeguate, l'intervento della Corte di Giustizia dell'UE è stato molto significativo. Infatti, nella decisione del 16 luglio 2020, C-311/18, la Corte ha interpretato congiuntamente l'art. 46 GDPR e l'art. 44 GDPR, affermando che l'art. 46 GDPR

> è contenuto nel capo V del [RGPD] e deve essere pertanto letto alla luce dell'articolo 44 di detto regolamento, rubricato «Principio generale per il trasferimento», il quale dispone che «[t]utte le disposizioni [di detto capo] sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal [medesimo] regolamento non sia pregiudicato». Tale livello di protezione deve, di conseguenza, essere garantito indipendentemente da quale sia la disposizione di detto capo sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo. (CGUE, 16 luglio 2020, C-311/18, § 92)

La Corte continua affermando che le:

> garanzie adeguate devono essere idonee a garantire che le persone i cui dati personali sono trasferiti verso un paese terzo sulla base di clausole tipo di protezione dei dati godano, come nell'ambito di un trasferimento fondato su una decisione di adeguatezza, di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione. (CGUE, 16 luglio 2020, C-311/18, § 96)

Poi, la Corte afferma che quando il trasferimento sia basato sulle clausole tipo adottate dalla Commissione *ex* art. 46, par. 2, lett. c) GDPR, le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti dall'art. 46 GDPR:

> devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest' ultimo, in particolare quelli enunciati all' articolo 45, paragrafo 2 (RGPD).

L'art. 45, par. 2 GDPR, come si è detto, individua gli elementi che la Commissione Europea deve considerare nel valutare l'adeguatezza del livello di protezione.

Dunque, l'uso degli strumenti previsti dall'art. 46, par. 2 GDPR non garantisce di per sé che i trasferimenti siano conformi al GDPR. Infatti, nella sentenza appena richiamata, (CGUE, 16 luglio 2020, C-311/18) la Corte ha anche affermato che l'adozione di clausole tipo non esclude che, al fine di garantire un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta, possa essere necessaria «in funzione della situazione esistente nell'uno o nell'altro paese terzo, l'adozione di misure supplementari da parte del titolare del trattamento» (§ 133).

5.3. Le deroghe in specifiche situazioni

In mancanza di una decisione di adeguatezza *ex* art. 45 GDPR, o di garanzie adeguate *ex* art. 46 GDPR, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'in-

teressato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; tale condizione non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; tale condizione non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri;

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; tale condizione non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri;

d) il trasferimento sia necessario per importanti motivi di interesse pubblico. In questo caso, l'interesse pubblico è riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento;

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri. Il trasferimento non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari.

Inoltre, se non è possibile basare il trasferimento su una decisione di adeguatezza o sull'esistenza di garanzie adeguate, e nessuna delle deroghe appena viste è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. In questo caso, il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14 GDPR (v. cap. *I diritti dell'interessato*), il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti. Ques'ultima possibilità di trasferimento non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

Infine, in mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare

espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri devono notificare tali disposizioni alla Commissione.

6. La riutilizzazione di dati personali detenuti da enti pubblici

La presa di consapevolezza sulle potenzialità derivanti dalla condivisione dei dati ha come primo punto di emersione la previsione di una disciplina di apertura dei dati e riuso delle informazioni del settore *pubblico*. Questo, come vedremo, si spiega secondo una logica molto semplice: mentre i dati del settore privato costituiscono generalmente un *asset* patrimoniale strumentale all'esercizio dell'attività d'impresa, secondo le logiche della concorrenza e della rivalità, viceversa i dati nella disponibilità dei soggetti pubblici non soggiacciono – di norma – a logiche di mercato. In altre parole, se la condivisione e il riuso dei dati nel settore privato si scontrano con le dinamiche dei vantaggi e degli svantaggi competitivi, nel settore pubblico la stessa operazione di «messa a disposizione» dei dati a soggetti terzi (pubblici o anche privati) assume i contorni di una esternalità positiva, ovvero di una azione non specificamente remunerata che produce di per sé effetti positivi sull'economia o sull'attività di altri soggetti.

6.1. La Direttiva *Open Data*

Esattamente a questa logica è ispirata la Direttiva *Open Data* 2019/1024 (recepita in Italia dal d.lgs. n. 200/2021 che ha emendato il d.lgs. 36/2006) che ha stabilito le regole per l'accesso e l'utilizzo dei dati pubblici da parte delle organizzazioni pubbliche e private all'interno dell'UE. La direttiva muove da alcune considerazioni che è qui utile riproporre:

> il *settore pubblico* degli Stati membri *raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni* in molti settori di attività, per esempio informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione. […] La *fornitura di tali informazioni* […] consente ai cittadini e alle persone giuridiche di *individuare nuovi modi di utilizzarle* e di *creare prodotti e servizi nuovi e innovativi.* (Considerando 8)

E ancora più chiaramente:

> l'*informazione del settore pubblico* rappresenta una fonte straordinaria di dati *in grado di contribuire a migliorare il mercato interno* e lo *sviluppo di nuove applicazioni per i consumatori e le persone giuridiche*. L'utilizzo intelligente dei dati, ivi compreso il loro trattamento attraverso applicazioni di intelligenza artificiale, può *trasformare tutti i settori dell'economia.* (Considerando 9)

Per conseguenza, la direttiva fissa un *principio generale* (art. 3) per il quale i 'documenti' in possesso di enti pubblici e imprese pubbliche siano riutilizzabili «a fini commerciali o non commerciali», siano messi a disposizione in un

«lasso di tempo ragionevole» (art. 4) a titolo, di regola, gratuito (art. 6), sempre salvo il rispetto della normativa in materia di protezione dei dati personali, di diritto d'autore e di proprietà industriale.

6.2. Il profilo pubblicistico del *Data Governance Act*

Con il *Data Governance Act*, definitivamente applicabile nell'Unione europea dal 24 settembre 2023, la logica del riutilizzo dei dati pubblici viene ulteriormente sviluppata, anche muovendo dalla constatazione degli scarsi risultati prodotti su questo piano dalla Direttiva *Open Data*:

> talune categorie di dati conservati in basi di dati pubbliche, quali dati commerciali riservati, dati soggetti a segreto statistico e dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali, *spesso non sono messe a disposizione*, nemmeno per attività di ricerca o di innovazione nel pubblico interesse, *nonostante tale disponibilità sia possibile in conformità del diritto dell'Unione applicabile*. (Considerando 6)

Il Regolamento perciò mira, nella sua parte dedicata al settore pubblico, a sbloccare quelle particolari categorie di dati soggetti a regimi speciali che ne impedivano la riutilizzazione, incoraggiando l'adozione di tecniche di anonimizzazione, aggregazione *et al.* dei dati protetti in maniera tale da assicurare il pieno rispetto dei diritti di terzi.

Il *Data Governance Act*, come accennato, fornisce per la prima volta alcune importanti definizioni, relative ai concetti di 'dato' (ovvero «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva»), di 'riutilizzo' del dato pubblico (ovvero il riuso «a fini commerciali o non commerciali»), di 'titolare dei dati' (ovvero chi «ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli»), di 'utente dei dati' (ovvero chi ha accesso ai dati e ha diritto di «utilizzare tali dati a fini commerciali o non commerciali») e di 'condivisione dei dati' (ovvero la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, dietro compenso o a titolo gratuito sulle qualificazioni soggettive all'interno del Data Governance Act, anche in relazione al GDPR v. cap. *Le definizioni fondamentali*).

Per quanto concerne il profilo pubblicistico, il Regolamento disciplina (art. 5) le condizioni per il riutilizzo di una o più delle categorie di dati protetti *ex* art. 3, par. 1 (cioè coperti da riservatezza commerciale, statistica, protezione dei diritti di proprietà intellettuale di terzi o protezione dei dati personali), detenuti da enti pubblici, prescrivendo che esse siano pubbliche, non discriminatorie, trasparenti, proporzionate e oggettivamente giustificate in relazione alle categorie di dati e alle finalità del riutilizzo e alla natura dei dati per i quali è consentito il riutilizzo.

In ogni caso, tali condizioni non debbono «limitare la concorrenza». Il Regolamento prevede (art. 6) che gli enti pubblici che consentono il riutilizzo delle

categorie di dati protetti di cui sopra possano imporre tariffe non discriminatorie, proporzionate, oggettivamente giustificate (in particolare, per l'eventuale trattamento applicato al fine di garantire i diritti dei terzi; *e.g.* anonimizzazione, aggregazione *etc.*) e che non limitino il gioco concorrenziale. La gestione è affidata ad un sistema di sportelli unici (art. 8), con articolazione settoriale, regionale o locale.

Ad ogni modo, è opportuno chiarire che il *Data Governance Act* non fissa alcun obbligo per gli enti pubblici di acconsentire al riutilizzo dei dati, ma stabilisce una serie di regole comuni che debbono applicarsi qualora l'ente, sia pure dietro compenso, decida di consentirne l'utilizzo.

L'ente pubblico può inoltre svolgere attività di fornitura di «servizi di intermediazione dei dati», nei termini di cui si dirà *infra*, e rivestire altresì il ruolo di 'titolare dei dati' ai sensi del Regolamento in esame, ovvero di quel soggetto a cui l'interessato può richiedere di mettere i propri dati, siano essi personali o non personali, a disposizione di un soggetto terzo, 'utente dei dati', che ha diritto di utilizzarli per finalità commerciali o non commerciali.

7. La condivisione e l'accesso ai dati del settore privato

Si è detto che la recente regolazione europea mira a liberare enormi quantità di dati a beneficio del mercato e dunque a favorire quanto più possibile la loro circolazione e condivisione nel rispetto dei diritti dei soggetti interessati e dei terzi a vario titolo coinvolti. Con molta più prudenza rispetto a quanto osservato per il settore pubblico, la disciplina di favore per la condivisione e l'accesso ai dati coinvolge anche il settore privato. In particolare, come si vedrà in appresso, l'Unione europea ha varato per lo più norme incentivanti la condivisione volontaria dei dati e solo in rare ed eccezionali occasioni ha previsto formule cogenti di accesso ai dati da parte dei soggetti pubblici o di soggetti terzi del mercato.

Proseguendo la nostra disamina, muoviamo verso il lato privatistico del *Data Governance Act*. In particolare, le fattispecie rilevanti sono quelle dei «servizi di intermediazione dei dati» e dell'«altruismo dei dati».

In entrambi i casi, il cuore della proposta è la condivisione dei dati secondo la logica della non rivalità e secondo il metodo della volontarietà: il Regolamento non introduce, come accennato già per il settore pubblico, alcun obbligo di condivisione, ma promuove e regolamenta le forme attraverso le quali tale condivisione può realizzarsi. In particolare, regole stringenti sono fornite in merito alle *Condizioni per la fornitura di servizi di intermediazione dei dati* (art. 12) e ai *Requisiti generali per la registrazione* in un registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute (artt. 17 ss.).

7.1. L'altruismo dei dati

L'altruismo dei dati mira a favorire la condivisione volontaria di dati *senza compenso* (salvo il rimborso dei costi sostenuti) per obiettivi di interesse generale (Capo IV del *Data Governance Act*).

L'obiettivo a tendere di questa legislazione di favore per la condivisione è perciò quello della creazione di «spazi comuni europei di dati», ossia «quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile» (considerando 27). L'art. 2, par. 1, n. 16), del *Data Governance Act* descrive l'altruismo dei dati come la «condivisione volontaria di dati sulla base del consenso accordato dagli interessati» o «sulle autorizzazioni di altri titolari dei dati», senza la richiesta o la ricezione di un compenso, salva la compensazione dei costi sostenuti.

Tale condivisione avviene, appunto, per fini altruistici, cioè per obiettivi di interesse generale, stabiliti nel diritto nazionale, 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.

Per poter concretamente realizzare tale possibilità di condivisione di dati personali e non personali, gli Stati membri saranno chiamati nei prossimi anni ad accreditare le «organizzazioni per l'altruismo dei dati» attraverso l'iscrizione in un registro pubblico nazionale. Ai sensi dell'art. 17 del *Data Governance Act*, tali organizzazioni non potranno perseguire scopi di lucro e dovranno, ai sensi degli artt. 20 e 21, assicurare un elevato livello di trasparenza in merito al trattamento di dati personali e all'utilizzo di dati non personali nonché assolvere a specifici obblighi di tutela assicurando che i dati siano sempre trattati per lo specifico fine altruistico per il quale sono stati condivisi.

7.2. I servizi di intermediazione dei dati

Come si è visto, il *Data Governance Act* favorisce la condivisione dei dati, personali e non, nella convinzione che più dati vengono condivisi fra enti pubblici e soggetti privati e fra gli stessi privati, maggiori sono le opportunità di sviluppo per l'economia europea.

In questo quadro, il legislatore eurounitario ha regolamentato una nuova tipologia di servizi, che cercano di affermarsi nella prassi: i servizi di intermediazione dei dati. Essi mirano a «instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei 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, n. 11), *Data Governance Act*).

Si tratta, dunque, di servizi che si prefiggono l'obiettivo di mettere in collegamento, da un lato, le persone fisiche cui i dati si riferiscono e i soggetti, diversi dagli interessati, che hanno il diritto di concedere a terzi l'accesso ai dati, anche non personali (i c.d. «titolari dei dati»: art. 2, n. 8, *Data Governance Act,* su cui v. *supra* cap. *Le definizioni fondamentali*, § 8.1) e, dall'altro, coloro che desiderano utilizzare tali dati (i c.d. «utenti dei dati»: art. 2, n. 9, *Data Governance Act,* su

cui v. *supra* cap. *Le definizioni fondamentali*, § 8.1). Il collegamento dev'essere diretto: non possono considerarsi, quindi, servizi di intermediazione dei dati quei servizi in cui il fornitore ottiene dati dai titolari per poi aggregarli, arricchirli o trasformarli, al fine di aggiungervi un valore sostanziale e concedere licenze per il loro utilizzo (art. 2, n. 11, lett. a).

L'intermediazione, inoltre, deve mirare all'instaurazione di un rapporto «commerciale» fra le due parti in questione e deve riguardare «un numero indeterminato di interessati e di titolari dei dati». Di conseguenza, tenendo conto del primo aspetto, tra i servizi in esame non rientrano i servizi di condivisione dei dati offerti da enti pubblici che agiscono per scopi diversi (art. 2, n. 11, lett. d)) e i servizi che si limitano alla messa a disposizione di strumenti tecnici per gli interessati o per i titolari dei dati per la condivisione di dati con altri (ad esempio, servizi di archiviazione sul *cloud*, di *web browser*, di posta elettronica), senza mirare né a instaurare un rapporto commerciale, né a consentire al fornitore di acquisire informazioni in merito all'eventuale instaurazione del rapporto commerciale (v. considerando 28, *Data Governance Act*). Valorizzando il secondo aspetto, occorre escludere dai servizi di intermediazione in esame quelli utilizzati da un titolare dei dati, o comunque all'interno di un gruppo chiuso di soggetti, al fine di garantire la funzionalità di oggetti o dispositivi connessi all'Internet delle cose (art. 2, n. 11, lett. c)). Infine, un'ulteriore esclusione si basa sull'oggetto dei servizi: se questo è rappresentato da «contenuti protetti da diritto d'autore», l'intermediazione non ricade nella definizione data dal legislatore europeo (art. 2, n. 11, lett. b)).

In concreto, tra gli esempi di servizi di intermediazione dei dati, il *Data Governace Act* cita: i mercati dei dati su cui le imprese possono mettere dati a disposizione di terzi, gli orchestratori di ecosistemi di condivisione dei dati aperti a tutte le parti interessate, nonché i *pool* di dati creati congiuntamente da più persone fisiche o giuridiche con l'intento di concedere licenze per il loro uso a tutte le parti interessate in modo che tutti i partecipanti che contribuiscono al *pool* siano ricompensati per il loro contributo (considerando 28).

Nell'ambito di tali servizi, meritano una menzione speciale i fornitori che hanno come obiettivo principale quello di aiutare gli interessati nell'esercizio dei loro diritti, riconosciuti dal GDPR, in relazione ai dati personali oggetto di trattamento da parte di terzi. Tali fornitori prendono il nome di «cooperative di dati» (v. art. 2, n. 15, *Data Governance Act*) nella misura in cui la struttura organizzativa sia costituita proprio da interessati, nei cui confronti – in quanto membri dell'organizzazione – la cooperativa interverrà in aiuto. Peraltro, tali cooperative di dati possono avere come membri anche piccole e medie imprese (PMI), che, laddove siano esercitate da enti collettivi (ad esempio, società commerciali), quindi soggetti diversi da persone fisiche, non sono certamente qualificabili come interessati al trattamento ai sensi del GDPR. Ciononostante, anche le PMI possono aver bisogno di un'organizzazione che le aiuti nell'esercizio dei loro diritti in relazione a determinati dati non personali.

Considerata l'importanza dei servizi di intermediazione dei dati, anche in ragione dei delicati interessi in gioco, il *Data Governance Act* sottopone la lo-

ro fornitura a una serie di condizioni stringenti tanto sul piano dei divieti (v. art. 12, lett. a), b) e, indirettamente, e)), quanto sul piano degli obblighi (v. art. 12, lett. c), d), f), g), h), i), j), k), l), m), n) ed o)), tra cui spicca l'obbligo di far sì che la procedura di accesso al servizio sia equa, trasparente e non discriminatoria sia per gli interessati e i titolari dei dati, sia per gli utenti dei dati, anche per quanto riguarda i prezzi e le condizioni di servizio. Inoltre, il fornitore di servizi di intermediazione dei dati può avviare la fornitura solo dopo aver presentato una notifica all'autorità competente, per i cui compiti, a livello nazionale, è designata come responsabile l'Agenzia per l'Italia Digitale (AGID) (art. 2, d.lgs. n. 144/2024).

8. I rapporti fra titolari, utenti e destinatari dei dati generati da «prodotti connessi» o «servizi correlati»

Il *Data Act* costituisce un'ulteriore disciplina che interviene nell'ambito della circolazione dei dati, ma, a differenza del *Data Governance Act*, non si limita a favorirne la condivisione attraverso pratiche volontarie, posto che impone, in determinati rapporti fra privati, specifici obblighi di accesso ai dati.

Inoltre, rispetto ad altre normative, il *Data Act* si distingue per il fatto di prendere in esame soltanto una peculiare tipologia di dati, ossia quelli generati dall'uso di un prodotto connesso a Internet (ad esempio, un dispositivo domotico o una macchina agricola intelligente) o di un servizio a esso correlato. Tali dati possono essere sia di natura *personale*, se forniscono informazioni ricollegabili a una persona fisica, sia di carattere *non personale*, se forniscono informazioni che non sono in grado di riguardare una persona fisica identificata o identificabile (ad esempio, le informazioni sui componenti di un suolo agricolo o sulla temperatura rilevata in una determinata area).

La generazione dei dati in esame è il risultato delle azioni di almeno due soggetti: il progettista o il fabbricante di un prodotto connesso, che in molti casi può essere anche un fornitore di servizi correlati, e l'utente del prodotto connesso o del servizio correlato (v. considerando 6 *Data Act*). Nonostante l'attività dell'utente sia fondamentale, nella prassi attuale è frequente che quest'ultimo, a causa del modo in cui i prodotti connessi sono progettati o delle misure di protezione adottate successivamente, non abbia accesso ai dati generati dall'uso di tali prodotti o servizi correlati, a meno che questi dati non siano dati personali cui poter accedere esercitando il diritto di cui all'art. 15 GDPR.

Per superare gli ostacoli della realtà appena descritta, il *Data Act* prevede che i dati in questione debbano essere resi accessibili all'utente (art. 3); qualora quest'ultimo non possa farlo direttamente a partire dal prodotto connesso o dal servizio correlato, il «titolare dei dati» deve mettere prontamente a disposizione dell'utente i dati, nonché i pertinenti metadati necessari per interpretare e utilizzare tali dati, senza indebito ritardo, con la stessa qualità di cui egli stesso dispone, in modo facile, sicuro e gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove

pertinente e tecnicamente possibile, in modo continuo e in tempo reale (art. 4, par. 1, *Data Act*).

Il «titolare dei dati», in quest'ambito, è definito come la persona fisica o giuridica che ha il diritto o l'obbligo, in base all'ordinamento europeo o nazionale, di utilizzare e mettere a disposizione dati, «compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato» (art. 2, n. 13), *Data Act*) (per un confronto di tale definizione con quella contenuta nel *Data Governance Act*, v. *supra* cap. *Le definizioni fondamentali*, § 8.1).

In casi particolari, il titolare dei dati può rifiutare una richiesta di accesso ai dati pervenuta dall'utente. Ciò può accadere quando: a) l'accesso ai dati possa compromettere i requisiti di sicurezza del prodotto connesso e comportare gravi effetti negativi per la salute, la sicurezza o la protezione di persone fisiche (art. 4, par. 2, *Data Act*); b) i dati in questione siano in grado di rivelare segreti commerciali del titolare e quest'ultimo possa dimostrare, sulla base di elementi oggettivi, che, a causa della divulgazione di tali segreti, subirebbe molto probabilmente gravi danni economici, anche se l'utente adottasse tutte le misure necessarie per tutelarne la riservatezza (art. 4, par. 8, *Data Act*).

Al di fuori di tali ipotesi, il titolare dei dati non solo deve concedere l'accesso all'utente, ma deve anche, se questi lo richiede, mettere a disposizione di terzi i dati che ottiene o può ottenere legittimamente dal prodotto connesso o dal servizio correlato, senza che ciò implichi uno sforzo sproporzionato che vada al di là di una semplice operazione (art. 5, par. 1, *Data Act*). I terzi in questione (ad esempio, imprese interessate a trattare i dati generati dai prodotti connessi per sviluppare servizi digitali innovativi), denominati «destinatari dei dati», devono di regola corrispondere al titolare dei dati un compenso, che verrà concordato con quest'ultimo insieme alle modalità di messa a disposizione dei dati.

Per entrambi i casi, le relative condizioni contrattuali devono essere eque, ragionevoli e non discriminatorie (v. artt. 8-9 *Data Act*). Invero, se una clausola contrattuale viene imposta unilateralmente dal titolare dei dati e si rivela essere abusiva, ossia di natura tale che il suo utilizzo si discosta considerevolmente dalle buone prassi commerciali in materia di accesso ai dati e relativo utilizzo, in contrasto con il principio di buona fede e correttezza, tale clausola non vincola (v. art. 13, parr. 1 e 3, *Data Act*). La novità di tale previsione è che essa consente di accertare l'abusività di una clausola – e dichiararne la conseguente nullità, secondo il diritto italiano – anche nei contratti tra imprese, e non solo nei contratti dei consumatori, per i quali già si applicano le norme in tema di clausole vessatorie contenute negli artt. 33 ss. cod. cons.

I diritti riconosciuti dal *Data Act* agli utenti integrano i diritti di accesso e alla portabilità dei dati di cui agli artt. 15 e 20 GDPR. Ad ogni modo, nell'eventualità di un conflitto tra il *Data Act* e il diritto dell'Unione in materia di protezione dei dati personali o la legislazione nazionale adottata conformemente a tale diritto dell'Unione, la prevalenza va accordata a queste ultime discipline (art. 1, par. 5, *Data Act*).

Riferimenti bibliografici

Angiolini, Chiara. 2020. *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*. Torino: Giappichelli.

Bachelet, Vittorio, Gianluigi Marino e Antonio Racano (a cura di). 2025. *Data Act. Accesso equo ai dati e loro utilizzo: profili sistematici e applicativi nell'orizzonte del diritto privato*. Wolters Kluwer.

Batlle, Sergi, van Waeyenberge, Arnaud. 2024. "EU-US Data Privacy Framework: A First Legal Assessment." *European Journal of Risk Regulation* 1.

Bravo, Fabio. 2021. "Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act." In *Contratto impresa e Europa* 1: 199-256.

Cuffaro, Vincenzo, D'Orazio, Roberto, Ricciuto, Vincenzo (a cura di). 2019. *I dati personali nel diritto europeo*. Torino: Giappichelli.

Proietti, Giuseppe. 2023. "Il trasferimento dei dati personali all'estero: proporzionalità, poteri delle agenzie di intelligence ed effetto Bruxelles." *Il diritto dell'Informazione e dell'informatica* 6.

Ricciuto, Vincenzo. 2022. *L'equivoco della privacy. Persona vs dato personale*. Napoli: Edizioni Scientifiche Italiane.