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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0021

La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa

Stefano Torregiani*

L'incremento esponenziale della circolazione dei dati dovuto all'avvento della digitalizzazione è stato accompagnato da un altrettanto rilevante aumento degli obblighi di localizzazione delle informazioni imposti dagli Stati membri dell'Unione europea. Il legislatore continentale, conscio dell'importanza che il libero flusso delle informazioni ricopre per la realizzazione del mercato unico digitale, ha reagito all'espansione dalla *data localization* attraverso una serie di interventi particolari e distinti, prevalentemente fondati sulla distinzione, non ancora del tutto pacifica, tra dati personali e dati non personali. Attraverso l'analisi delle similitudini e delle differenze che caratterizzano le principali fonti dell'ordinamento europeo in materia di dati, lo scopo del presente lavoro sarà quello di valutare se questo mosaico regolamentare, preferito ad un approccio onnicomprensivo, sia idoneo a disciplinare efficacemente lo spazio comune europeo dei dati.

Circolazione dei dati – Obblighi di localizzazione – Dato personale – Dato non personale

1. Introduzione

Il fenomeno della data driven innovation è diventato l'indiscusso protagonista dell'attuale realtà economica e sociale nel giro di pochissimi anni, trasformandosi nel punto di riferimento per qualsiasi modello di sviluppo economico e tecnologico. Attualmente, il vero potere si trova nelle mani di chi, tramite la gestione di una vastissima mole di dati, riesce ad estrarre valore e, conseguentemente, prendere decisioni economicamente molto vantaggiose, a fronte di costi assai ridotti[1].

Questo è il principale motivo alla base della repentina acquisizione di rilevanza da parte del bene "dato", il quale oggi si presenta come una risorsa economico-finanziaria di cui nessuna attività, né pubblica, né privata, può più fare a meno[2].

Uno degli aspetti più importanti concernenti l'innovazione digitale è quello relativo alla circolazione di queste informazioni: l'addestramento degli algoritmi, le analisi di mercato, l'elaborazione di strategie pubbliche, l'adozione di piani aziendali sono tutte attività che hanno come denominatore comune la stretta correlazione con il trattamento di una serie di dati che provengono da fonti diverse e, nella maggior parte dei casi, da Paesi diversi. In tal senso, dunque, la tematica del flusso di dati gioca un ruolo chiave in una realtà economico-giuridica che si contraddistingue per la sua globalità e per la rilevante presenza di catene di valore transfrontaliere[3].

Tuttavia, parallelamente alla diffusione dei dati ed alla loro circolazione, l'ultima decade ha registrato la proliferazione del suo antagonista, gli obblighi di localizzazione (fenomeno internazionalmente co-

*S. Torregiani è dottorando di ricerca in Scienze giuridiche presso l'Università degli Studi di Macerata nel curriculum Istituzioni e territorio nella dimensione nazionale, europea e internazionale. Questo saggio fa parte della Sezione monografica *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati* a cura di Simone Calzolaio.

nosciuto con il nome di *data localization*)[4]. Il loro numero è cresciuto di pari passo all'aumento dell'importanza dei dati per la società, giacché anche il dato risponde all'antica logica secondo cui più un bene ha valore, più è incline al rischio di offesa e, di conseguenza, richiede una maggiore tutela. Difatti, le principali ragioni che sono alla base dell'introduzione di misure legislative o amministrative da parte degli Stati a difesa del proprio patrimonio informativo riguardano la sicurezza interna, la facilità di accesso delle autorità nazionali alle informazioni necessarie alla vigilanza e lo sviluppo industriale domestico[5].

L'obiettivo del presente contributo è quello di valutare come le due tematiche interconnesse, ma contrapposte, della libera circolazione e della *data localization* siano state affrontate dal legislatore europeo tramite gli ultimi interventi in materia di *data law*. Come si avrà modo di vedere nel prosieguo, anziché affrontare il problema proponendo una soluzione unica ed onnicomprensiva, l'Unione europea ha preferito prima effettuare una distinzione di fondo tra dato personale e dato non personale per poi procedere all'adozione di due normative distinte che, malgrado comunicanti, rischiano di scostarsi troppo da una realtà digitale in cui tale distinzione è molto meno chiara di quanto la normativa lasci presupporre[6].

2. La reazione europea alla *data localization*

Di regola, con il termine *data localization* non ci si riferisce solo ed esclusivamente a quelle misure che impongono, direttamente o indirettamente, il luogo in cui deve essere effettuato un determinato trattamento, poiché vengono ricomprese anche quelle disposizioni che fissano vincoli più o meno stringenti al trasferimento dei dati al di là dei confini nazionali[7]. Questa circostanza allarga enormemente il novero delle misure che possono rientrare nella definizione, coprendo sostanzialmente tutti gli ordinamenti che hanno una disciplina in materia di circolazione dei dati, in quanto, quando non impongono un divieto generale oppure permettono il trasferimento solo dopo un primo trattamento a livello locale[8], si premurano comunque di prescrivere una serie di condizioni affinché i dati possano abbandonare il territorio di provenienza.

Alla luce di queste considerazioni, le restrizioni alla libera circolazione possono distinguersi in "rigide" o "condizionali"[9]. Le prime, le quali obbligano il titolare ad eseguire una determinata fase del trattamento localmente, si suddividono a loro volta in sottocategorie, a seconda della rigidità della misura: partendo da una disposizione che richiede il solo storage a livello locale – ossia mantenere una copia interna – e passando per quelle che, oltre all'archiviazione, impongono il processing domestico, si arriva fino al divieto generale di trasferimento, con la conseguenza che, al di fuori dei propri confini, è vietato persino il semplice accesso alle informazioni[10]. Le restrizioni condizionali, invece, lasciano sempre uno spazio, più o meno angusto, al trasferimento, ma lo rendono più gravoso giacché alcuni requisiti devono essere soddisfatti dal soggetto trasferente o dal ricevente, oppure da entrambi[11]. Tale distinzione si riflette anche sul bersaglio delle restrizioni: mentre quelle condizionali sono concepite al fine di limitare i trasferimenti di un determinato tipo di dato – generalmente personale –, quelle rigide hanno una dimensione prettamente settoriale, con la conseguenza che la distinzione tra dato personale e non personale non acquisisce alcuna rilevanza[12].

A dispetto dell'incremento massivo, la dottrina è sostanzialmente concorde nel valutare come negativi gli effetti prodotti dalla *data localization* nei confronti delle economie statali, giacché gli obiettivi di sicurezza, controllo e privacy che sono alla base dell'introduzione di simili misure restrittive potrebbero essere raggiunti tramite strade alternative capaci di apportare incalcolabili benefici al settore produttivo domestico[13]. Lo stesso discorso vale per un'organizzazione internazionale quale l'Unione europea che, dal canto suo, non è stata risparmiata da questa ondata di protezionismo che ha reso la *data localization* il principale attore non protagonista delle normative concernenti la gestione dei dati. Invero, più di uno studio sulle legislazioni vigenti nei singoli Stati membri dell'Unione ha dimostrato che, anche nel nostro continente, l'aumento del valore dell'informazione è stato accompagnato da un clima di sfiducia nelle normative e, soprattutto, nei sistemi di sicurezza degli altri Paesi membri, sfociando in poco tempo nell'emanazione di una serie di obblighi giuridici atti ad internalizzare il trattamento nella misura più ampia possibile[14].

Resosi conto di questa preoccupante tendenza, con l'inizio della seconda decade di questo secolo, il legislatore europeo ha deciso di prendere una posizione netta al riguardo, invertendo la rotta nel tentativo di ristabilire un clima di fiducia reciproca in tutto il continente. Con queste premesse nasce la strategia per la creazione del "Mercato Unico Digitale", concepito nelle intenzioni delle istituzioni europee come un passo imprescindibile affinché il mercato interno possa continuare a funzionare nell'era della digitalizzazione[15]. Oggi è, difatti, impossibile condurre un'attività economica con caratteri transfrontalieri senza far fronte a tutte le questioni connesse al tema

del trasferimento delle informazioni: i dati devono necessariamente muoversi assieme al bene al quale ineriscono, pertanto, in un mercato in cui gli ostacoli allo spostamento di persone, merci, capitali e servizi sono stati abbattuti, è chiaro che l'incentivo alla libera circolazione delle informazioni si manifesta come un passaggio irrinunciabile[16].

Tra l'altro, riuscire nell'intento di trasformare simili iniziative in disposizioni normative efficaci ed innovative rappresenta uno dei pochi ambiti in cui il vecchio continente può ancora imporsi quale capofila: se l'arretratezza tecnologica nei confronti dei giganti del tech che hanno le loro sedi nel Nord America e nell'Asia orientale non sembra potersi recuperare nel breve termine[17], agire per rendere il mercato continentale più appetibile rimane un dovere dell'Unione europea[18]. Segnatamente, i primi passi mossi dagli organismi dell'Unione verso la soppressione delle barriere virtuali alla libera circolazione, in favore di un incremento nell'utilizzo transfrontaliero delle informazioni, risalgono al 2011, quando la Commissione europea riconosce che le precedenti normative in materia di armonizzazione e di incentivo all'apertura nell'utilizzo dei dati nel settore pubblico – in particolare la Direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico – non hanno sortito gli effetti sperati e che, di fatto, le barriere allo scambio di informazioni pubbliche costituiscono ancora un peso per l'economia continentale[19]. Tuttavia, dati i tempi non ancora maturi per una discussione profonda come quella odierna, soprattutto per quanto riguarda la distinzione tra dato personale e non personale[20], il documento circoscrive i suoi riferimenti ai dati pubblici, salvo qualche sporadico accenno alla tutela della vita privata ed alla protezione dei dati personali[21].

Dopo un'ulteriore comunicazione del luglio 2014 in cui viene evidenziato il problema degli ostacoli alla libera circolazione dei dati ed il loro effetto frenante nei confronti dello sviluppo del *cloud computing* e dello sfruttamento dei big data[22], i documenti istituzionali del biennio 2017-2018 si focalizzano quasi esclusivamente sugli sforzi necessari alla creazione del mercato unico digitale. Secondo la visione europea, lo sviluppo di tutte le tecnologie basate sullo scambio di informazioni – dal *cloud computing*, all'*Internet of Things*, dalla *data analysis*, all'intelligenza artificiale – sono in grado di crescere e prosperare all'interno dell'economia continentale grazie a due pilastri fondamentali. Da un lato, la protezione dei dati personali, la quale, una volta aggiornata e consolidatasi nell'ordinamento europeo a tutti i livelli[23], promette di mantenere l'essere umano come centro gravitazionale attorno al quale si sviluppa la tecnologia, e non viceversa. Dall'altro lato, invece, si trova la libera circolazione dei dati, sia personali che non, la quale, accompagnata da una (non ancora del tutto) aggiornata disciplina riguardante l'interoperabilità e l'accesso alle informazioni, costituirà un incentivo senza eguali al progresso dell'economia europea.

Tuttavia, ciò che distingue l'ordinamento europeo dai regimi giuridici dei Paesi tecnologicamente più avanzati, è proprio la preponderanza che il primo dei due pilastri, la protezione dei dati personali, assume nei confronti della libera circolazione delle informazioni. Prendendo come termine di paragone due fra i Paesi leader dell'attuale panorama mondiale, negli Stati Uniti la regolamentazione riguardante le informazioni relative alle persone fisiche viene ancora percepita in un'ottica perlopiù consumeristica, con la conseguenza che l'individuo riesce ad ottenere protezione proprio in quanto consumatore, ma non in quanto persona che gode di un diritto fondamentale alla protezione dei propri dati[24]. Una impostazione altrettanto differente è invece quella riguardante la Repubblica popolare cinese, dove, in un certo senso, traspare una duplice concezione: se, per un verso, l'ordinamento cinese sembra si stia avvicinando a quello europeo nell'ambito delle relazioni fra privati, per altro verso, il precedente approccio centralizzato continua a caratterizzare la disciplina nei rapporti verticali fra individuo e governo, secondo un sistema autoritario e gerarchico che pone al vertice la sicurezza dello Stato[25].

Nell'ordinamento europeo, invece, il ruolo cardine attribuito alla persona fisica ed ai suoi diritti fondamentali rappresenta il principale motivo per cui l'impianto normativo dedicato alle altre dimensioni del *data law*, soprattutto, quella economica, si sia sviluppato in un secondo momento o, quantomeno, sia stato ipotizzato come sussidiario. Infatti, è dopo l'approvazione del Regolamento generale sulla protezione dei dati personali (GDPR)[26], precisamente nella Comunicazione sulla costruzione di un'economia dei dati europea del 2017, che è stata concepita l'idea di un regolamento specificamente dedicato ai dati a carattere non personale[27]. Effettivamente, dal testo emerge la ormai raggiunta consapevolezza che per lo sviluppo di un'economia sana e stabile non è sufficiente la sola tutela dell'individuo, poiché si rivela fondamentale anche mettere le imprese e le pubbliche amministrazioni in una posizione che dia loro la possibilità di essere promotrici di un nuovo modello economico-sociale[28]. Pertanto, la Commissione sottolinea quanto sia importante un approccio organico alla materia e chiarisce espressamente che il principio della libera circolazione dei dati all'interno dell'Unione, inteso quale corollario imprescindibi-

le delle altre libertà riconosciute nel mercato unico europeo, non riguarda solo i dati personali – come avviene nel GDPR – ma interessa tutte le tipologie di informazioni[29]. Tuttavia, subito dopo questa statuizione che potremmo definire pionieristica, interviene una ulteriore precisazione volta a rimarcare la differenza insita in quei regimi giuridici dei dati che attuano il medesimo principio di libera circolazione: mentre le norme concernenti il flusso dei dati possono essere il risultato di trattative con Paesi terzi, quelle relative alla protezione dei dati personali hanno uno status diverso, in quanto, godendo del rango di diritti fondamentali, non possono essere oggetto di negoziazione[30].

Un ulteriore documento finalizzato alla costruzione delle fondamenta del mercato unico digitale, in cui l'eterogeneità del regime giuridico europeo in materia di circolazione dei dati si avverte con maggiore evidenza, è la Comunicazione "Verso uno spazio europeo comune dei dati". In tal caso, lo scopo principale della Commissione risiede nella proposizione del cosiddetto *data package*, ossia di un insieme di tre provvedimenti che, in aggiunta alla normativa sulla protezione dei dati personali appena entrata in vigore ed al regolamento sulla circolazione dei dati non personali – all'epoca non ancora definitivamente approvato –, mira a creare "uno spazio comune dei dati nell'UE, un'area digitale senza soluzione di continuità, la cui scala consenta lo sviluppo di nuovi prodotti e servizi basati sui dati"[31].

La proposta della Commissione sfocia nell'adozione di tre documenti diversi che, nonostante non si traducano tutti in strumenti di *hard law*, di fatto predispongono o incentivano la creazione di regole differenti per i dati a seconda del settore in cui essi vengono trattati[32]. Se il primo strumento, ossia la direttiva relativa al riutilizzo dell'informazione nel settore pubblico, fa riferimento ad un ampliamento della politica di messa a disposizione dei dati definiti come "pubblici"[33], il secondo consiste in una Raccomandazione volta ad incentivare il regime di *open access* per i dati raccolti e trattati nell'ambito della ricerca scientifica[34]. Il terzo provvedimento, infine, riguarda gli orientamenti sulla condivisione dei dati nel settore privato, tramite i quali la Commissione si offre quale promotrice di principi, accordi e regole a cui gli operatori privati dovrebbero fare ricorso al fine di trasformare il mercato europeo in un grande *hub* di informazioni, da cui tutti potrebbero trarre beneficio[35]. Ciò che accomuna i tre provvedimenti è l'idea di una politica, o meglio, di una cultura di condivisione dei dati che non si limiti semplicemente al settore pubblico – già in parte destinatario di un'apposita direttiva – ma che riguardi anche il settore privato nei rapporti tra imprese e nei rapporti tra imprese ed enti pubblici. Peraltro, nonostante l'intenzione fosse quella di incentivare lo spostamento delle informazioni all'interno del territorio continentale nella misura più ampia possibile, è evidente che la vasta gamma di strumenti regolatori messi in campo dalle istituzioni europee rischia di produrre una settorializzazione e stratificazione normativa in grado di compromettere la libera circolazione[36].

3. La circolazione dei dati personali

3.1. All'interno dell'Unione europea

Come detto, la disciplina riguardante il flusso dei dati personali in Europa è frutto dell'evoluzione normativa che negli anni recenti ha elevato la tutela dell'individuo con riferimento al trattamento delle sue informazioni al rango di diritto fondamentale. Conseguentemente, l'impianto normativo è concepito in maniera tale che la tutela giuridica continentale rimanga il più a lungo possibile ancorata all'informazione, continuando a seguirla in ogni suo spostamento, come una garanzia che non può essere scissa dal bene al quale si accompagna[37]. Questo principio pervade l'intera normativa e, infatti, ha rappresentato uno dei capisaldi attorno ai quali sono state plasmate le disposizioni in materia di circolazione dei dati personali, sia dal punto di vista interno, ossia limitato al flusso intra-europeo, sia dal punto di vista esterno, quando i dati lasciano l'Unione.

Per quanto riguarda la circolazione tra gli Stati membri, con l'impiego della fonte regolamentare in luogo della precedente direttiva, il legislatore europeo è riuscito ad uniformare le discipline nazionali, cosicché, almeno teoricamente, ogni regime giuridico conforme al GDPR deve assicurare lo stesso livello di tutela[38]. Pertanto, alla luce della forte spinta verso l'armonizzazione in materia di protezione dei dati, l'articolo 1, paragrafo 3 del GDPR stabilisce che i singoli Stati membri non possono più lamentare una lacuna nella protezione di tali dati come motivo alla base dell'imposizione di un divieto di trasferimento al di fuori dei propri confini[39]. Invero, nonostante anche la precedente direttiva esordisse con parole simili, la mancata armonizzazione dovuta all'impiego di una fonte normativa "più debole" non era di fatto riuscita a limitare la propagazione degli obblighi di localizzazione dettati da motivi attinenti alla tutela della privacy delle persone fisiche. Anzi, proprio gli ultimi anni di vigenza della precedente direttiva sono stati testimoni di una proliferazione di restrizioni senza precedenti, non solo a causa dell'avvento della digitalizzazione, ma anche perché la promessa di un

elevato livello di protezione dei dati veniva utilizzata come giustificazione di tali misure[40].

Ad ogni modo, nonostante la libera circolazione non venga espressamente annoverata tra i principi fondamentali del GDPR, una chiara affermazione in tal senso proviene direttamente dalla Commissione europea la quale, nell'intento di allargarne l'applicazione anche ai casi in cui agli Stati membri è consentito disciplinare materie specifiche, afferma che questi "dovrebbero essere incoraggiati a non fare uso delle clausole di deroga del regolamento per limitare ulteriormente la libera circolazione dei dati"[41].

Tuttavia, se il Regolamento generale sulla protezione dei dati personali rappresenta un apparato giuridico che, oltre che tutelare l'individuo, è funzionale al contrasto dell'insorgenza degli obblighi di *data localization*, è opportuno rammentare che i mezzi attraverso i quali gli Stati membri sono in grado di introdurre nuove restrizioni, o mantenere quelle già esistenti, non ricadono tutti nell'ambito di applicazione del GDPR[42]. Mentre la protezione della privacy degli individui non può più fungere da scudo della localizzazione, i singoli Paesi possono ancora fare affidamento sulle deroghe previste da altre fonti settoriali del diritto europeo riguardanti la gestione dei dati[43], le quali dovranno comunque superare il vaglio relativo alla loro compatibilità con quanto stabilito dal diritto dell'Unione in materia di libertà fondamentali[44].

A tal proposito, non ci si può esimere dal sottolineare ancora una volta come la moltitudine di fonti normative europee, nel tentativo di regolamentare dettagliatamente la gestione dei dati, non faccia altro che offrire ulteriori opportunità per l'introduzione di impedimenti al libero flusso delle informazioni.

3.2. Al di fuori dell'Unione europea

Un discorso diverso vale, invece, se si rivolge lo sguardo alle modalità con cui l'Unione europea disciplina la circolazione dei dati al di fuori dei propri confini, poiché è lo stesso ordinamento giuridico continentale a trasformarsi in un parziale obbligo di localizzazione dei dati personali.

Il meccanismo di trasferimento di informazioni personali verso Paesi terzi o organizzazioni internazionali muove dalla precedente impostazione sancita dalla Direttive 95/46/CE, riadattandola al nuovo contesto digitalizzato in cui si trova ad operare e, soprattutto, cristallizzando le regole di origine giurisprudenziale elaborate dalla Corte di giustizia dell'Unione nella vigenza della normativa ormai abrogata[45]. Pertanto, affinché i dati personali possano lasciare il territorio europeo, gli articoli 44 e seguenti del GDPR predispongono una serie di condizioni in assenza delle quali il trasferimento non può avere luogo. Dunque, nonostante il legislatore abbia predisposto un ampio ventaglio di possibilità di trasferimento capaci di adeguarsi al tipo di situazione in cui versa il titolare del trattamento, stando alla definizione generale di *data localization*, anche l'ordinamento giuridico europeo rientra a pieno titolo nel novero di quelle misure atte a limitare la libera circolazione[46].

Il ragionamento alla base del divieto di imporre obblighi di localizzazione all'interno dell'Unione, viene in questo caso impiegato *a contrario* proprio per condizionare il trasferimento verso l'esterno: dal momento in cui la tutela dei dati personali è ben lontana dal poter essere considerata omogenea a livello globale, l'Unione europea ha deciso di introdurre un meccanismo che sia in grado, quantomeno nelle intenzioni, di agganciare al dato la tutela europea, anche quando questo esce dall'ordinamento giuridico di origine[47]. Se da un lato, le norme europee appaiono come un garanzia imprescindibile nel panorama globale, dall'altro lato, non sono mancate insinuazioni volte a sollevare dubbi sul vero scopo dell'Unione nel predisporre un meccanismo di trasferimento così dettagliato. Non potendo essere alla pari di altre realtà dal punto di vista dello sviluppo tecnologico[48], sembra che l'Unione stia cercando di recuperare terreno sotto l'aspetto della disciplina giuridica, attraverso una applicazione extraterritoriale delle proprie regole[49], le quali, è bene ricordarlo, devono essere osservate, non solo la prima volta che i dati abbandonano l'Europa, ma anche per i trasferimenti successivi[50].

Entrando nel dettaglio, si nota sin da subito come il Regolamento generale racchiuda una serie di regole in cui il flusso internazionale dei dati è percepito come un "elemento strutturale"[51] della normativa e non più, come accadeva nella Direttiva – in vigore in un momento storico in cui lo spostamento delle informazioni tra Stati non aveva la rilevanza che ha oggi – come circostanza episodica annoverabile fra le ipotesi delle mere eccezioni. Dunque, la disciplina che governa il meccanismo di trasferimento esordisce con il principio in ragione del quale i dati possono lasciare il territorio europeo solamente se rispettano le condizioni del capo V. Lungi dal prescrivere un divieto generale come le misure restrittive più rigide, la consapevolezza raggiunta dal GDPR in merito alla essenzialità del flusso internazionale dei dati lo colloca nel complesso degli obblighi di localizzazione condizionali più tenui fra quelli attualmente in vigore[52].

A conferma di ciò, è possibile constatare che se la decisione di adeguatezza, di cui all'articolo 45[53], rimane il metodo principe per il trasferimento come avveniva in precedenza[54], ora questo stesso stru-

mento viene potenziato poiché tanto il diritto europeo quanto quello nazionale non possono fissare limiti al trasferimento extra-europeo nei confronti di quei Paesi o organizzazioni internazionali il cui ordinamento giuridico è stato riconosciuto come adeguato[55]. Tale previsione si inserisce nel disegno generale promosso dal legislatore europeo verso quella che sembra essere una maggiore apertura del continente, con lo scopo di rafforzare le relazioni con altri Paesi, senza però sacrificare la tutela dell'individuo[56].

Un ulteriore aggiornamento concerne la nuova impostazione assunta dal GDPR in materia di deroghe. Se prima tutto ciò che ricadeva fuori dalla decisione di adeguatezza era classificato come deroga, oggi questa qualifica spetta solamente alle ipotesi specifiche – e più numerose rispetto al passato –[57] elencate nell'articolo 49[58]. Ciononostante, la predisposizione di un sistema derogatorio apparentemente a maglie più larghe, non si traduce in un lasciapassare volto ad eludere le disposizioni in materia di protezione di dati: il Comitato europeo per la protezione dei dati è intervenuto sul punto con delle apposite linee guida, insistendo sul fatto che l'interpretazione delle disposizioni all'articolo 49 deve essere la più restrittiva possibile[59].

Infine, sulla base della stessa logica innovativa sono state aggiornate le garanzie adeguate, ossia quelle misure per mezzo delle quali è possibile trasferire i dati personali verso un Paese terzo il cui ordinamento giuridico non è stato valutato come adeguato da parte della Commissione europea. Il sistema in vigore, oltre a risultare più centralizzato rispetto al passato grazie ai maggiori poteri di controllo preventivo ed autorizzatorio concessi agli attori istituzionali, dimostra ancora una volta la presa di coscienza da parte del Regolamento del fatto che il movimento dei dati da un continente all'altro sia diventato un elemento essenziale dell'economia moderna. Il GDPR riesce a bilanciare la tutela dell'individuo con la circolazione dei dati personali tramite la responsabilizzazione dei soggetti coinvolti, ossia titolari e responsabili del trattamento, i quali, siano essi mittenti o riceventi, devono definire misure negoziali o paranegoziali al fine di sopperire alle lacune del sistema giuridico applicabile[60]. Oltre all'impiego di clausole contrattuali tipo, codici di condotta, meccanismi di certificazione o altri strumenti vincolanti, una delle principali novità risiede nell'introduzione delle "norme vincolanti d'impresa" (*Binding Corporate Rules*, o BCRs)[61]. Mentre nel testo della Direttiva non erano affatto prese in considerazione[62], queste disposizioni sono state concepite al preciso scopo di favorire lo scambio di informazioni sia nei gruppi imprenditoriali che nei "gruppi di imprese che svolgono un'attività comune"[63], di fatto prevenendo la formazione di barriere alla libera circolazione di informazioni che ostacolerebbero non poco l'attività commerciale del gruppo. L'inserimento delle BCRs e l'aggiunta di un articolo a sé stante nel regolamento segnano una presa di posizione forte da parte dell'Unione europea poiché, dalla totale assenza nella normativa precedente, sono ora divenute un *unicum* nel panorama del trasferimento extra-europeo dei dati personali, differente da tutte le altre garanzie[64].

Ad ogni modo, il fatto che l'ordinamento giuridico europeo risulti essere una normativa moderna, attenta alle esigenze delle imprese che conducono attività a carattere transfrontaliero e più permissivo rispetto ad altri sistemi giuridici, non è sufficiente a precluderne la qualificazione di regime giuridico di *data localization*[65]. Oltretutto, questa situazione sembra destinata a permanere ancora a lungo, giacché, se la motivazione alla base di questa restrizione risiede nella tutela della privacy degli individui che in altri ordinamenti potrebbe risultare non adeguatamente salvaguardata, l'eventuale soppressione delle condizioni restrittive presupporrebbe il raggiungimento di un livello di armonizzazione globale che, ad oggi, sembra lontano[66]. Invero, dal momento che numerosi Paesi stanno virando verso un'impostazione giuridica in materia di tutela di dati e di localizzazione degli stessi non necessariamente simile a quella del vecchio continente, si può presumere che negli anni avvenire, anziché ad una omogeneizzazione della normativa, assisteremo all'acuirsi dell'arroccamento all'interno delle proprie fortezze informatiche da parte di Stati gelosi del proprio patrimonio digitale.

4. La circolazione dei dati non personali

Nella mente del legislatore europeo, il Regolamento relativo ad un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (RDNP)[67] nasce come strumento diretto a colmare le lacune insorte in seguito all'approvazione del GDPR, il quale, circoscrivendo il suo ambito di applicazione alla categoria dei dati personali, aveva lasciato senza copertura altre tipologie di informazione e i relativi obblighi di localizzazione[68]. Così, al termine di un iter durato all'incirca un anno, precisamente nel 2018, il Regolamento sulla libera circolazione dei dati non personali è stato approvato e a partire dal 28 maggio 2019 trova applicazione nel territorio europeo.

Prima di procedere alla valutazione dell'impatto che la nuova disciplina ha avuto ed avrà con riguardo alla circolazione delle informazioni, è doveroso fare due osservazioni preliminari. La prima è volta a for-

nire una definizione della nuova categoria del dato non personale. A tal proposito, non sembra essere sufficientemente esaustiva la sola lettura dell'articolo 3 del RDNP che, nel primo punto, afferma che i dati non personali sono quelli "diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679"[69]. Pertanto, consapevole delle problematicità giuridiche che di regola si accompagnano alle definizioni di carattere negativo, l'articolo 8, paragrafo 3 del RDNP, ha attribuito alla Commissione europea il compito di formulare ulteriori "orientamenti informativi" atti a specificare il regolamento. Conseguentemente, le linee guida pubblicate a maggio dello scorso anno in ossequio a suddetta disposizione si sono rivelate estremamente opportune, in quanto contenenti una definizione più puntuale della nozione di dato non personale che, invece, non è presente nel testo del Regolamento. Pertanto, grazie al lavoro della Commissione, è ora possibile affermare che la categoria "dato non personale" è costituita sia dalle informazioni che sin dall'origine non si riferivano a una persona fisica identificata o identificabile[70], sia dalle informazioni che, pur inizialmente personali, sono state anonimizzate in un secondo momento.

Peraltro, è pur sempre doveroso osservare che la scelta di demandare (quantomeno in parte) la definizione di questa nuova fattispecie ad un atto il cui valore giuridico all'interno dell'ordinamento europeo non può di certo essere equiparato a quello delle fonti regolamentari, potrebbe comportare seri problemi di coordinamento con altre normative continentali e, soprattutto, potrebbe mettere a rischio la certezza e l'applicazione uniforme del diritto nell'Unione europea. Le linee guida della Commissione, difatti, nonostante offrano un punto di vista autorevole per l'interpretazione del diritto europeo e, in quanto tali, risultino funzionali a risolvere alcuni problemi in chiave applicativa del RDNP, rimangono pur sempre prive della forza di legge che contraddistingue le disposizioni contenute nel regolamento[71]. L'indeterminatezza riguardante la questione definitoria corre il rischio di minare la coerenza di qualificazione del dato fra gli ordinamenti giuridici degli Stati membri, specialmente in quegli ambiti in cui ciò è reso più difficoltoso sia dalle potenzialità di re-identificazione offerte dagli sviluppi tecnologici[72], sia dai margini di discrezionalità lasciati ai singoli ordinamenti nazionali, come avviene nel caso dei dati relativi alle persone fisiche decedute[73]. Naturalmente, la poca chiarezza che attiene alla disposizione cardine della nuova disciplina non potrà che avere ripercussioni negative sulla distinzione, ben lungi dall'essere pacifica[74], tra dato personale e non personale e sull'applicazione dei due regolamenti europei[75].

La seconda osservazione, invece, mira a sottolineare la profonda differenza che intercorre tra il Regolamento generale sui dati personali ed il RDNP per quanto concerne la disciplina della circolazione delle rispettive categorie di informazioni. Se, a differenza di quanto fatto dal GDPR nei confronti dei dati personali, il RDNP è principalmente focalizzato sul tema della circolazione e dell'accesso delle autorità amministrative in una dimensione prettamente interna, la sorte che spetta ai dati non personali – che sfuggono all'applicazione del meccanismo condizionale previsto dagli articoli 44 e seguenti del GDPR – nell'ipotesi in cui essi vengano destinati verso Paesi terzi non sembra essere stata presa in debita considerazione[76]. Pertanto, se da un lato, salvo l'unica eccezione relativa alla pubblica sicurezza che si vedrà in seguito, il regolamento non sembra contenere disposizioni di *data localization*, dall'altro, la mancanza di riferimenti alla dimensione extraeuropea potrebbe incoraggiare lo spostamento di informazioni di inestimabile valore per lo sviluppo delle nuove tecnologie in ordinamenti giuridici che rispondono a regole diverse, incentivando, pertanto, lo sfruttamento di questi dati solamente all'estero, dove l'Unione europea non potrebbe né controllarli né trarne alcun beneficio[77].

Rivolgendo ora l'attenzione a quanto avviene all'interno del territorio continentale, è possibile osservare che il legislatore europeo ha deciso di incentivare la libera circolazione concentrando i propri sforzi, sia verso il settore pubblico, con l'abbattimento degli obblighi di localizzazione derivanti da legislazioni o pratiche amministrative in vigore negli Stati membri[78], sia verso il settore privato, tramite l'incoraggiamento della portabilità delle medesime informazioni nell'ambito delle attività degli utenti professionali[79], in maniera tale da prevenire le pratiche di *vendor lock-in* nemiche del mercato unico[80].

4.1. Il divieto degli obblighi di localizzazione

Il primo scopo che il RDNP intende conseguire è quello di eliminare le restrizioni ingiustificate alla libera circolazione dei dati non personali, considerate dalla Commissione europea il più grande ostacolo allo sviluppo dell'economia dei dati nell'Unione[81]. In virtù di ciò, la norma centrale del regolamento è l'articolo 4, paragrafo 1, il quale vieta agli Stati membri l'introduzione e il mantenimento di obblighi di localizzazione dei dati quando non giustificati da motivi di pubblica sicurezza[82]. Ai fini del Regolamento, sono identificati quali obblighi di localizzazione le disposizioni di legge, gli orientamenti o le pratiche amministrative che, direttamente o indirettamente,

impongono l'elaborazione o la conservazione dei dati limitatamente ad una determinata area geografica[83]. In particolare, i documenti degli organi europei fanno spesso riferimento alle richieste delle autorità di controllo di archiviare localmente i propri dati, alle regole del segreto professionale che prediligono il trattamento a livello locale, alle linee guida amministrative che dispongono lo stesso principio relativamente ai dati gestiti da enti pubblici e, non da ultimo, alle norme di settore che impongono l'utilizzo di dispositivi omologati in un determinato Stato membro[84].

L'identificazione di simili restrizioni risulta molto più complessa di quanto possa apparire a prima vista. Uno studio di particolare interesse, eseguito anteriormente all'adozione definitiva del Regolamento, tende a distinguere tra due diverse categorie[85]. *In primis*, ci sono le cosiddette "barriere dirette", individuabili in maniera più agevole, le quali includono tutte le misure normative che stabiliscono espressamente dove conservare – o non conservare – i dati oppure che contengono obblighi tali per cui il loro rispetto può essere garantito solo tramite la conservazione in un determinato territorio[86]. Più ardue da riconoscere sono, invece, le "barriere indirette". Queste comprendono quelle norme la cui interpretazione può ragionevolmente limitare la scelta di chi gestisce i dati per quanto riguarda il luogo di archiviazione ed il libero flusso. La maggiore difficoltà deriva dal fatto che l'obbligatorietà della restrizione, essendo strettamente correlata all'interpretazione, potrebbe non essere uniformemente intesa[87].

La categoria delle barriere indirette, nonostante i suoi confini piuttosto sfumati, non può essere affatto sottovalutata, dal momento in cui al suo interno si cela la maggioranza degli ostacoli alla libera circolazione dei dati non personali: lo studio citato giunge alla conclusione che, delle quaranta barriere totali rinvenute al termine dell'analisi, trenta rientrano proprio in questa categoria più "sibillina"[88]. In realtà, alla luce delle ipotesi analizzate[89], questo squilibrio non desta troppo stupore: la circostanza che i dati debbano, da un lato, essere obbligatoriamente resi disponibili ai titolari del trattamento o alle autorità di vigilanza, mentre, dall'altro, non possano essere resi noti a terze parti, unita ai troppo spesso frequenti obblighi di autorizzazione prescritti per poter utilizzare una determinata struttura di archiviazione o un determinato responsabile del trattamento[90], possono verosimilmente spingere chi accumula queste informazioni a preferire una soluzione domestica – e magari più costosa in termini di conservazione – in luogo di una più funzionale alla propria impresa, ma che potrebbe attirare attenzioni indesiderate da parte delle autorità di controllo.

Peraltro, la questione degli obblighi di localizzazione permette di individuare una significativa differenza del Regolamento sui dati non personali rispetto al GDPR. Mentre il regolamento riguardante i dati personali concentra la sua attenzione, in primo luogo, sui soggetti che intervengono nella filiera del trattamento dei dati – il titolare ed il responsabile del trattamento – stabilendo gli obblighi da rispettare al fine di assicurare una tutela efficiente al *data subject*, il RDNP dedica la sua norma cardine agli Stati membri. D'altronde, non potrebbe essere diversamente giacché, se per il GDPR l'obiettivo (primario) è quello di tutelare un diritto fondamentale dell'individuo, il secondo regolamento si inserisce, invece, in quella serie di strumenti che, incentivando la circolazione, mirano a rafforzare il mercato unico[91]. Ad ulteriore conferma del ruolo di destinatari principali della disciplina ricoperto dai Paesi membri, il testo del Regolamento tiene a precisare che la normativa non è volta né a ridurre le facoltà di scelta delle imprese in relazione alla localizzazione dei dati, le quali rimangono comunque libere di optare per una soluzione domestica[92], né ad imporre l'esternalizzazione dei servizi da parte degli enti pubblici quando sussistono esigenze che li spingono a preferire l'autofornitura[93].

Come anticipato, la presa di posizione dell'Unione europea nei confronti della *data localization* nell'ambito della circolazione dei dati non personali scaturisce dal preoccupante aumento di misure restrittive verificatosi negli ultimi anni, spesso dettato dalla convinzione che la conservazione e l'analisi dei dati all'interno dei confini nazionali siano sinonimo di sicurezza oppure che facilitino l'accesso e la sorveglianza da parte delle autorità. In aggiunta, alcune limitazioni sono state imposte al preciso scopo di sfavorire i fornitori di servizi stranieri o multinazionali rispetto a quelli nazionali[94]. Stando alle stime prettamente economiche presentate dalla Commissione europea, la drastica diminuzione di queste restrizioni voluta dal nuovo regolamento permetterebbe all'economia dei dati di crescere fino a 739 miliardi di euro entro il 2020[95]. Oltretutto, secondo uno studio dello *European Centre for International Political Economy* (ECIPE), l'effetto sarà più che positivo per il mercato, poiché, beneficiando le industrie di costi minori legati alla maggiore flessibilità nella gestione dei propri dati, il PIL potrebbe crescere di circa 8 miliardi di euro l'anno[96]. Pertanto, la Commissione, al fine di cogliere le opportunità offerte dall'economia dei dati, ha ritenuto necessario garantire il libero flusso delle informazioni stabilendo il medesimo principio di libera circolazione, ma garantendolo tramite due fonti diverse, il GDPR, per il versante

dei dati personali ed il RDNP, per quello dei dati non personali[97]. Sebbene offrano un quadro all'apparenza nitido, le valutazioni della Commissione si focalizzano quasi esclusivamente sull'aspetto economico connesso all'aumento delle misure restrittive alla circolazione dei dati, senza tuttavia approfondire ulteriori profili che meritano di essere presi in considerazione. In tal senso, alcune delle ultime iniziative promosse tanto a livello europeo[98], quanto a livello nazionale[99], non sembrano avere come obiettivo una riappropriazione del bene "dato" in chiave monopolistica e con l'intento di escluderne gli altri dal *management* ma, al contrario, tentano con non poche difficoltà di riconquistare il terreno perduto dagli ordinamenti giuridici nazionali e sovranazionali in un ambito, quello della gestione dei dati a valenza strategica, in cui la posizione centrale un tempo ricoperta è stata fortemente ridimensionata dall'entrata in campo dei servizi offerti dagli OTT[100]. Pertanto, se per un verso, il gravame economico derivante da simili politiche è innegabile, per altro verso, la questione della *data localization* potrebbe essere riletta come un timido tentativo attuato dalle istituzioni del vecchio continente di stabilire un regime concorrenziale con riguardo al trattamento dei dati, attraverso la realizzazione di infrastrutture proprie che siano in grado di operare parallelamente a quelle ben più avanzate dei giganti del tech.

4.1.1. La sicurezza pubblica come unica eccezione

L'articolo 4 del Regolamento sulla libera circolazione dei dati non personali prevede come unica eccezione al divieto di imporre obblighi di localizzazione la sicurezza pubblica. Al fine di evitare l'insorgere o il permanere di discipline non fondate su tale base legittima, grava sugli Stati membri il dovere di procedere alla disamina di tutte le norme che impongono un obbligo di localizzazione per poi abrogare quelle non conformi al Regolamento. Tuttavia, nel caso in cui ritengano necessario il mantenimento di alcune misure restrittive, proprio perché fondate su motivi di pubblica sicurezza, devono darne comunicazione alla Commissione europea allegando la relativa giustificazione[101]. Per contro, alla Commissione è riconosciuta la facoltà di presentare osservazioni qualora ritenga opportuno che tali disposizioni debbano essere modificate o addirittura abrogate, in quanto non confacenti ai principi sanciti dal diritto comunitario[102] o dalla giurisprudenza della Corte di giustizia dell'Unione[103].

Il considerando n. 19 del RDNP agevola l'interpretazione del significato di sicurezza pubblica. Innanzitutto, il riferimento alla sicurezza sia interna che esterna permette di trattenere tutte le informazioni potenzialmente utili ai fini di prevenzione di attacchi provenienti da Paesi terzi, di fatto legittimando la conservazione di dati relativi a contesti non nazionali o non europei. Appare in tal caso evidente il legame con la speciale disciplina antiterrorismo diffusasi in tutto il continente a seguito degli attacchi terroristici degli anni recenti. Come evidenziato dalla dottrina, il timore di essere vittime di simili aggressioni ha scatenato la proliferazione di normative *ad hoc* che hanno eroso alcuni diritti fondamentali degli individui – soprattutto il diritto alla protezione dei dati personali – in nome della pubblica sicurezza[104]. *A fortiori*, un simile atteggiamento potrebbe contraddistinguere la regolamentazione dei dati non personali: scevro da rischi di lesione diretta ai diritti fondamentali della persona fisica, lo Stato tenterà di trattenere nelle proprie banche dati quante più informazioni possibili, legittimato dall'interesse alla difesa delle "questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati"[105].

Nel prosieguo, la normativa sembra ampliare di molto il novero di interessi legittimanti una deroga. Difatti, nell'esigere una minaccia "reale e sufficientemente grave ad uno degli interessi fondamentali della società", vengono espressamente riportati "il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari".

In questa definizione a prima vista dettagliata, potrebbero nascondersi non poche insidie interpretative: basti pensare al concetto di servizio pubblico essenziale, il quale, non godendo di una definizione uniforme a livello continentale[106], rischia di creare una disparità di trattamento tra i diversi Stati membri. Altrettante incertezze accompagnano le nozioni di incolumità pubblica e interessi militari. Se la prima può potenzialmente impedire la circolazione di numerose informazioni relative alla salute dei cittadini – già oggetto di significative barriere indirette secondo lo studio sopra citato –[107], gli interessi militari, a loro volta, tolgono dalla circolazione, non solo le informazioni *latu sensu* strategiche, ma anche la maggior parte dei dati relativi alla produzione di materiale utilizzato dalle forze armate, detenuti dalle industrie belliche.

Se questi sono i presupposti, è probabile che gli Stati membri, desiderosi di mantenere le informazioni più delicate nel territorio in cui possono esercitare un potere "diretto", daranno un'interpretazione

estensiva al concetto di sicurezza pubblica, al preciso scopo di limitare la fuoriuscita dei dati nella misura più ampia possibile. A tal riguardo, sono condivisibili le perplessità espresse dal Comitato economico e sociale europeo (CESE) con riferimento alla imprecisione con cui viene delineata questa nozione ed alla mancanza di un "riferimento alle controversie o alle modalità per verificare in che modo gli Stati membri rispetteranno i criteri della pubblica sicurezza, né ad eventuali sanzioni nei loro confronti, ove opportuno"[108].

Quanto detto assume particolare rilevanza a fronte del contesto in cui operano alcune agenzie governative, reso noto a seguito delle rivelazioni riguardanti la vicenda *Datagate*[109]. Questa esperienza ha dimostrato che ad essere interessati al possesso di dati non sono solamente le compagnie private, ma anche le agenzie di intelligence che, proprio al fine di garantire la sicurezza pubblica, si sono rese protagoniste di una raccolta massiva di informazioni mai vista nella storia[110]. È bene notare che, nonostante il dibattito manifestatosi in seno all'opinione pubblica a partire dal 2013 si sia concentrato sulla violazione della vita privata degli individui sottoposti a sorveglianza, le stesse osservazioni potrebbero essere svolte, *mutatis mutandis*, in relazione ai dati a carattere non personale. Ne è un esempio significativo il comprovato meccanismo in voga fra i funzionari degli organi inquirenti consistente nel chiedere accesso alle informazioni detenute da imprese private nel settore ICT. Richieste che nella maggior parte dei casi non trovano nessuna base giuridica riconosciuta dalla legge e che, solitamente, vengono assecondate per motivi di reverenza o per timore di ripercussioni negative[111].

In un certo senso, sussiste la possibilità che, grazie allo schermo della sicurezza pubblica, possa venire alla luce anche per i dati non personali una differenziazione già nota per quelli personali. Se il Regolamento generale assicura una disciplina giuridica parzialmente diversa – *rectius*, più stringente – per le cosiddette categorie particolari di dati[112], è plausibile che in futuro si andrà a delineare una distinzione simile anche per i dati non personali. Riprendendo la vecchia nomenclatura tanto cara al nostro legislatore[113], una sorta di dato non personale "sensibile", ossia un dato che per la sua connessione funzionale con l'interesse collettivo della sicurezza pubblica, giustifica un regime giuridico diverso, grazie al quale lo Stato può imporre all'ente che lo conserva, pubblico o privato che sia, un obbligo di localizzazione[114].

In ultima analisi, essendo ancora nella fase iniziale di vigenza del RDNP, l'ampiezza dell'area che il concetto di pubblica sicurezza andrà concretamente a ricoprire verrà definita dalla prassi degli Stati membri e, soprattutto, dall'evoluzione giurisprudenziale della Corte di giustizia dell'Unione europea, la quale, al fine di dare corpo alla nuova normativa, potrebbe ridurre la discrezionalità interpretativa riconosciuta dal regolamento.

4.2. Una nuova portabilità autoregolamentata

A seguito della risonanza che il diritto alla portabilità dei dati personali ha avuto con l'entrata in vigore del GDPR, anche per il Regolamento sui dati non personali viene sottolineato sin da subito l'impatto positivo che il libero trasferimento delle informazioni da un fornitore di servizi ad un altro, su richiesta dell'utilizzatore e senza costi eccessivi, potrebbe avere nei confronti della concorrenza nel mercato interno[115]. Inoltre, è lo stesso testo della nuova disciplina che effettua una comparazione fra il diritto già vigente nell'Unione – in particolare il GDPR – che garantisce una tutela solida al consumatore desideroso di cambiare il prestatore di servizi, e le lacune che, al contrario, riguardano la situazione in cui versano gli utenti professionali, i quali, sprovvisti di una simile protezione, spesso si trovano intrappolati a causa di pratiche di *vendor lock-in* che comportano oneri di mantenimento più alti ed, al contempo, danneggiano la competitività delle imprese[116].

Sfortunatamente, malgrado le premesse, per il particolare caso dei dati a carattere non personale il legislatore europeo ha deciso di intraprendere una strada diversa rispetto a quanto fatto nel 2016[117]: se alle persone fisiche è riconosciuto a livello normativo un vero e proprio diritto alla portabilità, gli utenti professionali possono solo fare affidamento sull'elaborazione di codici di condotta di autoregolamentazione che, benché supportata e controllata direttamente dalla Commissione, non riuscirà mai a garantire quella certezza del diritto e quella parità di condizioni che dovrebbero essere alla base dell'adozione di questo regolamento[118]. Oltretutto, è difficile comprendere perché ragioni quali la necessità di "mantenere il passo con la potenziale innovazione del mercato e tener conto dell'esperienza e delle competenze dei fornitori di servizi e degli utenti professionali di servizi di trattamento di dati"[119], possano giustificare una regolamentazione tramite codici di condotta in luogo di un vero e proprio diritto che sia in grado di bilanciare lo squilibrio di potere intercorrente tra tali utenti professionali, spesso piccole e medie imprese, e fornitori di servizi online, i quali con la digitalizzazione dei settori pubblico e privato, stanno velocemente trasformandosi negli attori più potenti del mercato[120].

La volontà del regolamento di distaccarsi in maniera netta dalla posizione adottata nel GDPR è di-

mostrata, prima che dalla predisposizione di una tutela giuridica più debole, anche dall'utilizzo di una terminologia differente: se l'individuo può fare affidamento sulla *portability* inglese o sulla *portabilité* francese, i codici di condotta devono essere orientati alla disciplina, rispettivamente, del *porting* o del *portage*[121]. Questa differenza terminologica deriva, probabilmente, dalla volontà di sottolineare in maniera chiara il tipo di relazione giuridica che viene presa in considerazione nei due testi. Il diritto alla portabilità di cui all'articolo 20 del GDPR fa riferimento ad una situazione giuridica in cui i due protagonisti sono, da un lato, l'interessato persona fisica e, dall'altro, colui che tratta le sue informazioni, il quale, di regola, incarna la figura del titolare del trattamento. Dunque, similmente a quanto si è visto nella tradizione statunitense[122], questo diritto si inserisce in un'ottica di tutela del consumatore nel rapporto con il fornitore del servizio[123]. Per i dati non personali, al contrario, l'articolo 6 circoscrive il suo riferimento non ad un utente generalmente inteso, bensì alla specifica categoria dell'utente professionale, il quale tratta i dati per fini connessi alla sua attività. Di conseguenza, il rapporto intercorrente tra l'utente professionale ed il fornitore di servizi di gestione di dati, più che in una dinamica B2C, può essere ricondotto nell'ambito business-to-business[124], similmente a quanto avviene nel caso di dati personali tra titolare del trattamento e responsabile del trattamento[125].

Ad avviso di chi scrive, la strategia che l'Unione europea ha deciso di perseguire appare discutibile. La necessità, più volte richiamata, del coinvolgimento delle PMI nel processo di elaborazione di questi codici di condotta non è uno strumento sufficientemente forte da dissuadere i dubbi che pervadono la preferenza per l'autoregolamentazione, soprattutto alla luce dell'attuale momento storico del mercato dei dati in cui poche grandi imprese stanno guadagnando capacità egemoniche. In questo frangente, l'Unione europea ha l'opportunità di distinguersi ancora una volta rispetto ad altre realtà giuridiche tramite una presa di posizione forte verso il riequilibrio di quella parità contrattuale che sembra essersi fortemente indebolita[126]. Proprio da tali esigenze sono di recente nate numerose istanze in ambito accademico volte a sollecitare un dibattito profondo sulla necessità di allargare la normativa a tutela del consumatore al fine di ricomprendere anche le piccole e medie imprese, così da scongiurare la formazione di posizioni dominanti che rischiano di alterare la libera concorrenza nel mercato europeo in modo irreversibile[127]. La prevenzione di pratiche simili potrebbe avvenire in maniera più efficace se solo il Regolamento fosse sceso più nel dettaglio, magari fissando a chiare lettere alcune delle norme inderogabili che i codici di condotta dovrebbero necessariamente includere oppure, come ha notato il CESE, definendo gli orientamenti da cui i meccanismi di autoregolamentazione dovrebbero muovere, non limitandosi al semplice richiamo alle migliori pratiche, agli obblighi informativi ed alle tabelle di marcia[128].

5. I punti deboli dell'impianto regolamentare europeo

Come si è avuto modo di vedere, l'ultimo decennio ha visto l'Unione europea assumere un ruolo centrale nel campo della regolamentazione del settore dei dati, attraverso una serie di iniziative che hanno gradualmente dato forma al mosaico del mercato europeo digitale. Tuttavia, le soluzioni di compromesso e le ampie lacune emerse al termine dell'iter legislativo che ha portato alla approvazione della disciplina del flusso dei dati non personali mostrano l'incompletezza di questo grande disegno[129].

In particolare, alcuni dei punti deboli della normativa in esame derivano da un contrasto che, benché preso in considerazione dal legislatore, non sembra essere stato risolto con una scelta adatta alle problematiche che titolari, responsabili del trattamento e gestori dei dati in genere si trovano ad affrontare quotidianamente. I regolamenti, le direttive e tutte le altre fonti, anche di *soft law*, adottate al fine di rendere l'economia dei dati alla portata di tutti sembrano essere lontane da una realtà dei fatti poliedrica ed interconnessa come quella odierna, con la conseguenza che quando differenti mondi entrano in contatto l'uno con l'altro tutto l'impianto normativo viene messo a dura prova.

Una chiara ipotesi in cui il Regolamento sui dati non personali sembra vacillare riguarda gli "insiemi di dati misti". Nonostante non vi sia una definizione esplicita nel Regolamento[130], sono considerati come tali quei dataset che sono composti sia da dati personali che da dati non personali. Il RDNP dedica a tale fattispecie il secondo paragrafo dell'articolo 2, il quale stabilisce che il Regolamento generale sulla protezione dei dati personali e quello sulla libera circolazione dei dati non personali si applicano alla rispettiva categoria di dati. Tuttavia – aggiunge la norma – quando tali insiemi sono "indissolubilmente legati"[131], il GDPR troverà applicazione nei confronti dell'intero dataset anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme[132], in ossequio alla costante logica della protezione prima della circolazione.

Il fenomeno in oggetto non sembra essere stato approfondito in maniera soddisfacente né dal Rego-

lamento, che, eccetto il riferimento alle valutazioni ed agli orientamenti della Commissione europea[133], gli dedica un solo paragrafo; né dalla Commissione stessa che nell'elaborazione di quelle linee guida che avrebbero dovuto semplificare il lavoro degli operatori del settore, si limita ad affermare che, in considerazione della diminuzione del valore derivante dalla eventuale separazione dell'insieme in dati personali e non personali, dell'assenza di una obbligo che imponga tale separazione e, soprattutto, del fatto che tali insiemi rappresentano la maggioranza dei dataset esistenti, il GDPR si applicherà, di regola, a tutti gli insiemi di dati misti[134].

In realtà, la vera falla del sistema da cui sembra provenire l'approccio, in un certo senso "sbrigativo", che traspare tanto dal testo del Regolamento quanto dalla guida della Commissione, può essere rinvenuta nel differente peso attribuito al concetto di rischio nei due regolamenti, il quale, creando un dislivello alla base delle normativa europea in materia di dati, contribuisce a rendere fragile l'intera struttura. Se il *risk-based approach* costituisce uno degli elementi qualificanti il Regolamento generale sui dati personali[135], la stessa cosa non può dirsi con riferimento alla disciplina dei dati non personali, dove la valutazione del rischio, che si rivelerebbe uno strumento assai utile per comprendere la natura del dato e per individuare le implicazioni che i dati non personali possono avere sull'insieme di dati misti, non viene presa in dovuta considerazione[136]. Difatti, la decisa accelerazione della digitalizzazione della società moderna ha messo in crisi la definizione stessa di dato personale, portando con sé innumerevoli difficoltà nell'individuazione della linea di confine tra carattere personale e non personale e causando non pochi disagi tanto ai titolari del trattamento quanto alle autorità di controllo che devono monitorarli. Pertanto, in un mondo dove la natura delle informazioni cambia frequentemente, non è più possibile limitare la valutazione del rischio – generalmente inteso e non limitato esclusivamente alla c.d. "valutazione d'impatto sulla protezione dei dati" prevista dall'art. 35 del GDPR – alle sole ipotesi di dati personali, ma appare opportuno, se non necessario, estenderla a tutti i dati che il medesimo soggetto ha a disposizione, includendo anche quelli non personali[137]. Purtroppo, è proprio l'assenza di una visione onnicomprensiva capace di tenere conto della mutevolezza della realtà digitale a minare l'efficacia delle disposizioni del RDNP, le quali non riescono a soddisfare l'esigenza di coordinamento con il Regolamento generale sui dati personali.

Questo particolare deficit potrebbe ripercuotersi negativamente sulla effettività della libera circolazione di tutti i tipi di informazione sia all'interno che all'esterno dell'Unione. In primo luogo, risultano evidenti le problematicità che dovrebbe affrontare il titolare del trattamento desideroso di usufruire delle possibilità offerte dal RDNP giacché, malgrado l'assenza di un obbligo diretto di separazione del dataset, si vedrebbe costretto a scindere il suo insieme in due parti: una costituita da dati personali che, ipoteticamente, potrebbe essere sottoposta ad una misura restrittiva della circolazione – motivata da ragioni diverse dalla protezione dei dati – mentre l'altra parte, contenente dati non personali, potrebbe essere trasferita liberamente[138]. Di conseguenza, graverebbe sul titolare del trattamento un onere aggiuntivo ed implicito che, prescrivendo di fatto un'operazione costosa e di difficile riuscita[139], rischia di incentivare quell'atteggiamento di chiusura che il Regolamento mira ad eliminare[140].

In secondo luogo, l'interpretazione fornita dalla Commissione che, nel tentativo di dare precedenza alla tutela dei dati personali, propende per un'applicazione aprioristica del regime più restrittivo previsto dal GDPR nei confronti degli insiemi dei dati misti, potrebbe condurre ad un'ulteriore barriera indiretta alla libera circolazione dei dati non personali, trasformandosi in buona sostanza proprio in una misura di *data localization*[141].

In ultima analisi, la delicatezza del problema degli insiemi di dati misti e le difficoltà nel gestire le conseguenze di una regolamentazione così scarna si possono osservare anche con riferimento alla questione della portabilità, dove la predisposizione di una tutela a due livelli suscita alcune perplessità. Innanzitutto, se i codici di condotta non riconosceranno un vero e proprio diritto di portabilità, l'utente professionale intenzionato a spostare presso un nuovo *provider* l'intero insieme, senza procedere ad una complicata separazione, rischierebbe di dover affrontare un lungo contenzioso con il precedente fornitore del servizio i cui tempi di risoluzione sono del tutto inconciliabili con la velocità a cui procede la società digitale[142]. Oltretutto, anche nell'ipotesi in cui venisse riconosciuto dai codici di condotta e da clausole contrattuali, la prevalenza di una prerogativa di questo genere non può essere data per certa nell'eventualità in cui dovesse entrare in conflitto con altri diritti espressamente stabiliti dalla lettera della legge[143], in particolare con quelli più maturi e radicati nel mondo digitale – ad esempio, la proprietà intellettuale, i segreti commerciali o i diritti connessi alla tutela giuridica delle banche dati[144].

6. La necessità di una visione onnicomprensiva per la realtà digitale moderna

L'economia globale ed interconnessa che caratterizza la nostra epoca si basa su un incessante scambio di informazioni che partono ed arrivano in tutte le parti del mondo in tempi praticamente nulli. In risposta al rapido aumento del valore economico e dell'importanza strategica dei dati, sia personali che non, si è assistito ad una crescita del sentimento di sfiducia fra gli Stati, sfociato poi nell'adozione di normative aventi ad oggetto obblighi di localizzazione. Di fronte ad un cambiamento di simile portata, l'ordinamento giuridico europeo ha deciso fronteggiare la sfida posta dal fenomeno della *data localization* non attraverso un'iniziativa singolare ed unica, ma seguendo un percorso a tappe, in linea con la gerarchia di valori della tradizione giuridica continentale. In prima battuta, il legislatore ha deciso di predisporre una tutela elevata all'interno dell'Unione europea per quanto riguarda il trattamento dei dati personali. Partendo da tale presupposto, ha poi elaborato un insieme di regole che, per un verso, incentivasse la circolazione di tali dati sul suolo continentale e, per l'altro, permettesse alla tutela di viaggiare con il dato personale anche quando questo viene trasferito verso Paesi terzi.

La disciplina riguardante l'altro versante del *data law*, quello del dato non personale, ha visto la luce in un secondo momento, quando il peso della mancanza di una normativa completa a sostegno dell'economia europea dei dati non era di fatto più sostenibile. Sfortunatamente, il Regolamento sulla libera circolazione dei dati non personali non sembra avere soddisfatto le aspettative, in quanto non riesce a fornire un quadro normativo sufficientemente aderente alle dinamiche della realtà digitale.

Allargando lo sguardo all'impianto generale in materia di dati, la critica principale che può muoversi nei confronti del legislatore europeo concerne la carenza di una risistemazione in chiave organica di tutta la disciplina. Attualmente, l'ordinamento continentale consta di una vasta gamma di normative settoriali e, in alcuni casi, non coordinate, la cui stratificazione nel corso dell'ultimo decennio rischia di confondere l'interprete e di tradursi in uno strumento non adatto a servire lo sviluppo della società digitale[145]. Le lacune patite dal Regolamento sui dati non personali non rappresentano altro che il precipitato ultimo di questa disordinata ipertrofia normativa: nonostante l'apparente complementarietà, le sue disposizioni sono state concepite come facenti parte di un *corpus* separato rispetto al Regolamento generale sulla protezione dei dati personali, in evidente contrasto con quella visione di insieme che è ormai imprescindibile se si vuole regolamentare il mondo virtuale con la speranza di ottenere risultati concreti. Viceversa, il RDNP rischia di diventare un regolamento senza oggetto in quanto l'assenza di una impostazione sistemica che tenga conto della preponderanza degli insiemi di dati misti e, soprattutto, delle caratteristiche dei soggetti che trattano questi insiemi, non permette di inquadrare il problema nella prospettiva idonea ad attribuire al dato non personale l'importanza che merita. In aggiunta, oltre alla prevalenza schiacciante del GDPR patita dal Regolamento sui dati non personali, non sono da sottovalutare le ulteriori problematiche di coordinamento di questi due regolamenti con le altre discipline settoriali che, spesso, prescindono dalla distinzione personale-non personale[146].

La risoluzione degli interrogativi che inevitabilmente emergono da questa confusione normativa è posta totalmente a carico del soggetto che gestisce i dati, il quale, disorientato in un labirinto di regole, si rifugerà nei lidi più sicuri, ma anche più costosi, dell'internalizzazione del trattamento dei dati. Tuttavia, è bene ricordare, simili pratiche non sono economicamente sostenibili da parte delle piccole e medie imprese che, ancora una volta, saranno costrette a pagare le conseguenze di disposizioni normative non coordinate adeguatamente fra loro.

Note

[1] OCSE, *Data-driven innovation. Big data for growth and well-being*, OCSE Publishing, Parigi, 2015.

[2] A. McAfee, E. Brynjolfsson, *Big data: the management revolution*, in "Harvard Business Review", 2012, n. 10.

[3] H.A. Ünver, G. Kim, *Cross-border data transfers and data localization*, EDAM Cyber Policy Paper Series, 2016, n. 3, p. 2-6.

[4] M. Bauer, H. Lee-Makiyama, E. Van der Marel, B. Verschelde, *The cost of data localisation: friendly fire on economic recovery*, ECIPE occasional paper, 2014, n. 3, p. 3-10.

[5] M.F. Ferracane, *Restrictions on cross-border data flows: a taxonomy*, ECIPE working paper, 2017, n. 1, p. 6.

[6] M.L. Montagnani, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in "Mercato concorrenza regole", 2019, n. 2, pp. 311-313.

[7] M.F. Ferracane, *op. cit.*, p. 2-3.

[8] Come, ad esempio, accade in Russia. Per un approfondimento, si veda A. Savelyev, *Russia's new personal data localization regulations: a step forward or a self-imposed sanction?*, in "Computer Law & Security Review", 2016.

[9] M.F. Ferracane, *op. cit.*, p. 2-3.

[10] *Ibidem.*

[11] *Ibidem.* Naturalmente, la realtà dei fatti non rispecchia così nettamente la classificazione appena svolta, giacché le differenze possono essere molto più labili di quanto si pensi, ed

anche una misura condizionale può facilmente tramutarsi in rigida se l'iter necessario ad addivenire al trasferimento è troppo oneroso per la dimensione in cui opera il trasferente.

[12] *Ivi*, p. 8-9.

[13] M. Bauer, H. Lee-Makiyama, E. van der Marel, B. Verschelde, *The cost of data localisation: friendly fire on economic recovery*, cit., p. 5-10.

[14] P.S. Ryan, R. Falvey, S. Merchant, *When the cloud goes local: the global problem with data localization*, in "Computer", Vol. 46, 2013, n. 12, p. 54-59; A. Chander, U.P. Le, *Breaking the web: data localization vs. the global internet*, Working Paper, 2014, n. 1, p. 10-16; European Commission, *Cross-border data flow in the digital single market: study on data location restrictions* (SMART n. 2015/0054), Publication Office of the EU, 2017.

[15] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Strategia per il mercato unico digitale in Europa* - COM(2015) 192 final, pp. 15-21.

[16] La relatrice del Parlamento europeo Anna Maria Corazza Bildt, a seguito dell'approvazione del Regolamento (UE) 2018/1807, ha affermato che è stata introdotta una "quinta libertà di circolazione" che riguarda tutti i dati.

[17] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti* - COM(2017) 228 final, 2017, pp. 23-26.

[18] M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, ECIPE policy brief, 2016, n. 3, pp. 12-13. In particolare: «A ban on data localisation is a powerful political message that the Single Market is open for business. This argument is particularly pertinent as the EU seeks to convince the market and turn the tide on the digital investments, and both inward and domestic investments into Europe's digital economy are withheld or diverted to other regions».

[19] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Dati aperti, un motore per l'innovazione, la crescita e una governance trasparente* - COM(2011) 882 final, pp. 7-8. In particolare: «Nonostante l'armonizzazione minima introdotta dalla direttiva del 2003 sul riutilizzo delle informazioni del settore pubblico, permangono differenze significative nelle norme e pratiche nazionali, con conseguente frammentazione del mercato interno dell'informazione e presenza di ostacoli alla creazione di servizi di informazione transfrontalieri».

[20] A tal proposito, è opportuno ricordare che, nonostante la tematica dei dati personali stesse prendendo piede, la prima proposta ufficiale emanata dalla Commissione con riguardo alla riforma della disciplina della protezione dei dati personali è datata gennaio 2012.

[21] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Dati aperti, un motore per l'innovazione, la crescita e una governance trasparente*, cit., pp. 5-6.

[22] Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Verso una florida economia basata sui dati* - COM(2014) 442 final, pp. 12-13.

[23] Per un'analisi dettagliata del percorso che ha condotto all'istituzionalizzazione del diritto alla protezione dei dati personali, si vedano: G. Gonzalez Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014; G.F. Aiello, *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation*, in "Osservatorio del diritto civile e commerciale", 2015, n. 2.

[24] L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in "diritticomparati.it", 2014, pp. 8-13.

[25] Per un approfondimento, si vedano: H. De Hert, V. Papakonstantinou, *The data protection regime in China. In-depth analysis for the LIBE Committee*, Publication Office of the EU, 2015, p. 13-27; Z. Yuexin, *Cyber protection of personal information in a multi-layered system*, in "Tsinghua China Law Review", 2019, n. 1.

[26] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE.

[27] C. Colpaert, M.-C. Janssens, *Work in progress: the proposal of the free flow of non-personal data regulation*, KU Leuven - CITIP Blog, 2018.

[28] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea* - COM(2017) 9 final, pp. 9-14.

[29] *Ivi*, pp. 2-5.

[30] *Ibidem*.

[31] Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Comunicazione "Verso uno spazio comune europeo dei dati"* - COM(2018) 232 final, p. 1.

[32] M.L. Montagnani, *op. cit.*, pp. 298-302.

[33] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

[34] Raccomandazione (UE) 2018/790 della Commissione del 25 aprile 2018 sull'accesso all'informazione scientifica e sulla sua conservazione.

[35] Commissione europea, *Documento di lavoro dei servizi della Commissione. Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Verso uno spazio comune europeo dei dati"* - SWD(2018) 125 final.

[36] M.L. Montagnani, *op. cit.*, pp. 298-302.

[37] S. Kirschen, *Il trasferimento all'estero dei dati*, in R. Panetta (a cura di), "Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018", Giuffrè, 2019, pp. 265-268.

[38] Regolamento (UE) 2016/679, considerando n. 13. In particolare: «Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione

non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

[39]Regolamento (UE) 2016/679, art. 1, par. 3: «La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

[40]M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, cit., p. 3-8.

[41]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea*, cit., pp. 5-8.

[42]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union* - COM (2019) 250 final, p. 15, dove è riportato un esempio eloquente al riguardo: «Una normativa nazionale prevede che la contabilità del personale sia situata in uno specifico Stato membro per ragioni riguardanti il controllo regolamentare, ad es. da parte dell'amministrazione fiscale nazionale. Tale normativa nazionale non rientrerebbe nell'ambito di applicazione dell'articolo 1, paragrafo 3, del regolamento generale sulla protezione dei dati, in quanto i motivi non riguardano la protezione dei dati personali. Questo obbligo dovrebbe invece essere valutato sulla base delle disposizioni relative alle libertà fondamentali e delle deroghe consentite a tali libertà previste nel trattato sul funzionamento dell'Unione europea».

[43]Gli esempi generalmente riportati fanno riferimento, ma non sono limitati, a: Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno; Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[44]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 14-15.

[45]Tra le sentenze più significative, si ricordano: Corte di Giustizia UE, 13 maggio 2014, causa C-131/12; Corte di Giustizia UE, 6 ottobre 2015, causa C-362/14; Corte di Giustizia UE, 28 luglio 2016, causa C-191/15. Per una panoramica generale sull'evoluzione della giurisprudenza della Corte di giustizia, si veda: S. Calzolaio, voce *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", Utet giuridica, 2017, pp. 620-624.

[46]Institute of International Finance, *Data flows across borders. Overcoming data localization restrictions*, 2019.

[47]Commissione europea, *Comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato* – COM(2017) 7 final, pp. 4-6. In particolare: «L'obiettivo principale di tali norme è garantire che, quando i dati personali dei cittadini europei vengono trasferiti all'estero, la tutela viaggi con loro».

[48]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti*, cit., pp. 23-26.

[49]V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in "Il diritto dell'informazione e dell'informatica", 2015, n. 4-5, pp. 683-695; L. Valle, L. Greco, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in "Il diritto dell'informazione e dell'informatica", 2017, n. 2, pp. 198-201; S. Kirschen, *op. cit.*, pp. 265-268.

[50]Regolamento (UE) 2016/679, art. 44.

[51]S. Kirschen, *op. cit.*, pp. 261-265.

[52]M.F. Ferracane, *op. cit.*, p. 5.

[53]Regolamento (UE) 2016/679, art. 45, par. 1: «Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche».

[54]S. Kirschen, *op. cit.*, pp. 261-272; L. Valle, L. Greco, *op. cit.*, pp. 188-191.

[55]Infatti, l'articolo 49, paragrafo 5 del GDPR recita: «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 notificano tali disposizioni alla Commissione». S. Kirschen, *op. cit.*, pp. 283-291.

[56]*Contra*, L. Valle, L. Greco, *op. cit.*, pp. 218-219. In particolare: «[...] per quanto concerne l'altro profilo della regolazione transfrontaliera dei dati personali relativo al trasferimento verso Paesi terzi esso è legato a dei canoni, come quello del controllo dell'adeguatezza della disciplina del Paese terzo e della decisione sull'adeguatezza di clausole standard da parte della Commissione europea, che poco si adattano ad un flusso di dati quale quello che si reputa conveniente allo sviluppo delle attività economiche nel mondo contemporaneo».

[57] S. Kirschen, *op. cit.*, pp. 283-291.

[58]L'elenco delle deroghe di cui all'articolo 49 del GDPR ricomprende: il consenso esplicito dell'interessato, l'esecuzione o la conclusione di un contratto in cui l'interessato è parte o beneficiario, importanti motivi di interesse pubblico, difesa o esercizio di un diritto in sede giudiziale, interessi vitali, quando le informazioni sono contenute in un registro aperto alla consultazione pubblica e, infine, interessi legittimi cogenti del titolare del trattamento.

[59]European Data Protection Board (EDPB), *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 2018. Invero, il Comitato, forzando il significato letterale del testo, afferma che i concetti di "occasionalità" e "non ripetitività" indicati con riferimento alla sola eccezione relativa agli interessi legittimi cogenti del titolare del trattamento, devono essere applicati a tutte le ipotesi previste nell'articolo, anche se non indicato esplicitamente.

[60]S. Kirschen, *op. cit.*, pp. 274-283.

[61]L'articolo 4, punto 20, del GDPR definisce le norme vincolanti d'impresa come «le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune». Pertanto, tali norme sono

costituite da quell'insieme di regole, politiche e strumenti applicabili (solamente) all'interno delle società del gruppo al fine di assicurare il rispetto dei principi, dei diritti e degli obblighi riguardanti la protezione dei dati personali nell'Unione europea. Per un approfondimento si veda, G.M. Riccio, *Model contract clauses e corporate binding rules: valide alternative al safe harbor agreement?*, in G. Resta, V. Zeno-Zencovich (a cura di), "La protezione transnazionale dei dati personali. Dai «Safe Harbour Principles» al «Privacy Shield»", Tre Press, 2016.

[62]Tuttavia, il loro impiego non era sconosciuto prima dell'avvento del GDPR, tanto che il Gruppo di lavoro Articolo 29 si era già espresso a tale riguardo nel 2003: Article 29 Data Protection Working Party (WP29), *Working document: transfers of personal data to third countries: applying article 26 (2) of the EU data protection directive to binding corporate rules for international data transfers* (WP74).

[63]S. Kirschen, *op. cit.*, pp. 274-283.

[64]*Ibidem*.

[65]Per una visione critica (e metaforica) del meccanismo europeo, si veda: A. Mantelero, *From "safe harbour" to "privacy shield". The "medieval" sovereignty on personal data*, in "Contratto e Impresa/Europa", 2016, n. 1.

[66]C. Focarelli, *Privacy. Proteggere i dati personali oggi*, Il Mulino, 2015, pp. 123-175.

[67]Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[68]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea*, cit., pp. 5-8.

[69]A tal proposito, è doveroso osservare che, nonostante il considerando 9 del Regolamento sembri accennare ad una definizione concreta della nozione di dato non personale, il suo carattere meramente esemplificativo non permette di trarre conclusioni inequivocabili al riguardo.

[70]Gli esempi riportati dalla Commissione sono quelli dei dati sulle condizioni meteorologiche prodotti da sensori o i dati sulle esigenze di manutenzione delle macchine industriali.

[71]Lo stesso documento sottolinea sin da subito il carattere puramente informativo della guida della Commissione: «Il presente documento è fornito dalla Commissione europea esclusivamente a titolo informativo. Esso non contiene alcuna interpretazione autorevole del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, né costituisce una decisione o un'opinione della Commissione europea. Tale documento non pregiudica eventuali decisioni o opinioni della Commissione europea, né le competenze della Corte di giustizia dell'Unione europea per l'interpretazione del regolamento conformemente ai trattati dell'UE».

[72]S. Stalla-Bourdillon, *A. Knight, Anonymous data v. personal data – A false debate: an EU perspective on anonymization, pseudonymization and personal data*, in "Wisconsin International Law Journal", 2017, n. 2; G. D'Acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, 2017.

[73]Il GDPR, come indicato al considerando 27, esclude i dati dei deceduti dal suo ambito di applicazione ma, al contempo, permette ai singoli Stati membri di adottare una scelta differente, disciplinando questo tipo di informazioni alla stregua di quelle a carattere personale (come avviene in Italia, ex art. 2-terdecies, d.lgs. 30 giugno 2003, n. 196). Di fatto, la discrezionalità riconosciuta ai singoli legislatori nazionali, legittimando una classificazione normativa differente dello stesso tipo di informazione, potrebbe portare alla creazione di ambiti normativi non totalmente coincidenti all'interno dell'unico ordinamento giuridico europeo.

[74]S. Calzolaio, voce *Protezione dei dati personali*, cit., pp. 605-608; S. Forge, *Optimal scope for free-flow of non-personal data in Europe*, IPOL, 2016, p. 1-6; I. Grae, R. Gellert, M. Husovec, *Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation*, in "European Law Review", 2019, n. 5, p. 605-621.

[75]M.L. Montagnani, *op. cit.*, pp. 304-310.

[76]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 15-16. In particolare: «Il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea non riguarda gli obblighi di localizzazione di dati imposti dagli Stati membri sull'archiviazione dei dati non personali in un paese terzo, che possono essere presenti negli ordinamenti giuridici nazionali».

[77]*Parere del Comitato economico e sociale europeo (CESE) sulla "Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"* - 2018/C 227/12, p. 6. In particolare: «Inoltre, la proposta della Commissione non tiene debito conto della natura globale e transeuropea dell'economia digitale e si preoccupa solo di regolamentare il mercato interno, dimenticando che quest'ultimo si sviluppa in un mercato globale, senza alcuna garanzia che gli altri paesi e continenti seguano le stesse regole che essa stessa intende attualmente applicare e senza il potere di imporle nei negoziati internazionali».

[78]Regolamento (UE) 2018/1807, considerando n. 4.

[79]La figura dell'"utente professionale" è definita dal punto 8, dell'articolo 3 del Regolamento come: «una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione».

[80]Regolamento (UE) 2018/1807, considerando n. 6.

[81]European Commission, *Staff working document impact assessment, Accompanying the document "Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union"* - SWD (2017) 304 final, part 1/2.

[82]L'articolo 4, rubricato *Libera circolazione dei dati all'interno dell'Unione*, al paragrafo 1 stabilisce: «Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità. Il primo comma del presente paragrafo fa salvo il paragrafo 3 e gli obblighi di localizzazione dei dati stabiliti sulla base del diritto vigente dell'Unione».

[83]Regolamento (UE) 2018/1807, art. 3, punto 5.

[84]European Commission, *Commission staff working document impact assessment. Accompanying the document "Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union"*, cit.

[85]European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. Questo studio molto approfondito identifica gli obblighi di localizzazione che si possono trovare in alcuni Stati membri dell'Unione europea, p. 18.

[86]A titolo esemplificativo, possono essere citate due fra le più recenti barriere dirette introdotte dal legislatore italiano. La prima è contenuta nel d.l. 21 settembre 2019, n. 105,

recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica» convertito in l. 18 novembre 2019, n. 133, il quale, tramite la creazione di un perimetro di sicurezza nazionale cibernetica, potrebbe limitare la circolazione di informazioni inerenti all'esercizio di "una funzione essenziale dello Stato" oppure alla "prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale». La seconda barriera, invece, può rinvenirsi nell'art. 6 del d.l. 30 aprile 2020, n. 28 convertito in l. 25 giugno 2020, n. 70, recante «Misure urgenti per l'introduzione del sistema di allerta Covid-19», che istituisce una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti che usufruiscono della app "Immuni". Per un approfondimento, si rinvia a S. Calzolaio, *Sistema di allerta Covid-19. Osservazioni sull'art. 6, d.l. 28/2020*, in E. Calzolaio, M. Meccarelli, S. Pollastrelli (a cura di), "Il diritto nella pandemia. Temi, problemi, domande", Macerata EUM, 2020.

[87] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. Lo studio tiene comunque a precisare che le barriere indirette sono state considerate tali alla luce delle valutazioni fatte da esperti del settore.

[88] *Ivi*, p. 6.

[89] *Ibidem*.

[90] *Ivi*, p. 103. Nello specifico, lo studio recita: «More numerous were the indirect data location requirements, which included the accessibility of data to specific supervisors or regulators, the definition of generic technical requirements, prior authorisation schemes for infrastructure or service providers, the mandatory use of a specific infrastructure, data segregation requirements, subcontracting restrictions, and data destruction requirements».

[91] Merita evidenziare che, mentre il Regolamento generale sulla protezione dei dati personali ha come base giuridica l'articolo 16 TFUE, il Regolamento relativo alla libera circolazione dei dati non personali è stato adottato sulla base dell'articolo 114 TFUE, il quale attribuisce al Parlamento ed al Consiglio la competenza ad adottare «le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno».

[92] Regolamento (UE) 2018/1807, considerando n. 4. In particolare: «Il presente regolamento non limita in alcun modo la libertà delle imprese di stipulare contratti che stabiliscano dove devono essere localizzati i dati. Il presente regolamento è inteso unicamente a salvaguardare tale libertà garantendo che il luogo stabilito possa trovarsi ovunque nell'Unione».

[93] Regolamento (UE) 2018/1807, considerando n. 14. In particolare: «Mentre le autorità pubbliche e gli organismi di diritto pubblico sono incoraggiate a considerare i vantaggi economici e di altro tipo dell'esternalizzazione a fornitori esterni di servizi, essi potrebbero avere ragioni legittime per scegliere l'autofornitura di servizi o l'internalizzazione. Di conseguenza, il presente regolamento non obbliga in alcun modo gli Stati membri a subappaltare o esternalizzare la fornitura di servizi che essi intendono fornire direttamente o organizzare con mezzi diversi dagli appalti pubblici».

[94] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. p. 17. In particolare: «These barriers can of course take many forms. In some cases, there is a clear and objective compliance requirement behind them, such as a legal obligation to store data locally in order to maintain national control over essential systems and services. In other cases, a barrier can result from business requirements (e.g. customer demand to store data locally), policy preferences (e.g. a desire to keep data within one's own jurisdiction), operational needs (e.g. a requirement to be able to destroy data), or even personal preferences (e.g. favouring local companies) and personal concerns (e.g. concern that foreign entities may seize data stored abroad)».

[95] IDC, Open Evidence, *European data market study*, Final Report (SMART 2013/0063), 2017.

[96] M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, cit.

[97] Regolamento (UE) 2018/1807, considerando n. 10. In particolare: «Il regolamento (UE) 2016/679 e il presente regolamento forniscono un insieme coerente di norme che disciplinano la libera circolazione di diversi tipi di dati».

[98] La proposta congiunta lanciata dai Ministeri dell'economia tedesco e francese di creare una infrastruttura digitale di matrice europea, denominata GAIA-X, rispondente ai valori continentali di sicurezza e tutela dei dati è evidentemente diretta a ridurre la dipendenza nei confronti dei fornitori di servizi non europei e ad incentivare la concorrenza. In tal senso, *GAIA-X: A pitch towards Europe. Status report on user ecosystems and requirements*, Federal Ministry for Economic Affairs and Energy (BMWi), 2020.

[99] La predisposizione di una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti della app "Immuni" nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19 rappresenta una chiara presa di posizione da parte del legislatore italiano, il quale ha preferito una soluzione con titolarità pubblica e con infrastrutture localizzate sul territorio nazionale. Per un approfondimento, si rinvia a: C. Colapietro, A. Iannuzzi, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, in "Dirittifondamentali.it", 2020, n. 2.

[100] A tal proposito, eloquente è il caso dei *Community Mobility Reports* messi a disposizione da Google per fornire una panoramica della variazione degli spostamenti della popolazione durante la pandemia causata dal Covid-19, i quali dimostrano quanto sia pervasiva e vasta la raccolta e l'analisi dei dati realizzata dai servizi OTT.

[101] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. 21. La medesima procedura è prevista al paragrafo 2 nell'eventualità in cui gli Stati intendano introdurre un nuovo obbligo dello stesso tenore.

[102] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. 21.

[103] Per le sentenze della Corte di giustizia dell'Unione europea più rilevanti a tale riguardo, si rinvia alla European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 13.

[104] M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in "federalismi.it", 2016, n. 23.

[105] Regolamento (UE) 2018/1807, considerando n. 19. A tale riguardo, il rischio di difformità nelle normative degli Stati membri che potrebbe derivare da questa facoltà di deroga si aggiunge a quello dovuto alla scelta, da parte del legislatore, di ricorrere allo strumento della direttiva per disciplinare il trattamento dei dati personali effettuato da autorità pubbliche in ambito penale. In particolare, ci si riferisce alla Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali

ed alla Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

[106] L. Tarantino, *Promozione della concorrenza e disciplina dei servizi pubblici*, 2016, pp. 8-11; A. Di Giovanni, *I servizi di interesse generale tra poteri di autorganizzazione e concessione di servizi*, Giappichelli, 2018, pp. 1-17.

[107] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit.

[108] *Parere del CESE sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"*, adottato il 25 settembre 2019.

[109] M. Nino, *Il caso "Datagate". I problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in "Diritti umani e diritto internazionale", 2013, n. 3, pp. 735-737.

[110] C. Focarelli, *op. cit.*, pp. 10-16.

[111] C. Kuner, F.H. Cate, C. Millard, D.J.B. Svantesson, *Systematic government access to private-sector data redux*, in "Articles by Maurer Faculty, Indiana University", 2014, n. 4. Due eccezioni degne di nota sono quelle di Microsoft ed Apple che si sono opposte alle richieste di accesso da parte delle autorità statunitensi, si veda M. Rubechi, *op. cit.*, p. 23.

[112] Ci si riferisce all'articolo 9 del Regolamento (UE) 2016/679, rubricato *Trattamento di categorie particolari di dati personali*.

[113] Prima dell'abrogazione, la Legge n. 675 del 31 dicembre 1996 relativa alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, all'articolo 22, riportava la rubrica "Dati sensibili". Anche il Decreto legislativo 30 giugno 2003, n. 196, riportava la medesima dicitura prima della modifica ad opera del decreto legislativo 101 del 2018 relativo alle disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

[114] Un concetto simile è presente nell'ordinamento giuridico della Repubblica popolare cinese dove viene in rilievo la nozione di *important data*, la quale, benché possa comprendere sia dati personali che non, appronta una disciplina più rigida proprio in virtù della particolare importanza di queste informazioni in riferimento alla sicurezza, all'economia o alla stabilità sociale del Paese. A questo proposito, si veda Z. Yuexin, *op. cit.*, p. 159-169.

[115] Regolamento (UE) 2018/1807, considerando n. 29.

[116] European Commission, *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy. Accompanying the document Communication Building a European data economy* - SWD(2017) 2 final, p. 46-49.

[117] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 18-21.

[118] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[119] Regolamento (UE) 2018/1807, considerando n. 30.

[120] *Parere del CESE sulla "Comunicazione della Commissione*, cit. Per un'analisi dettagliata del diritto alla portabilità che ne include gli eventuali effetti negativi, anche se con riferimento ai dati personali, si veda: P. Swire, Y. Lagos, *Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique*, in "Maryland Law Review", 2013, n. 2, p. 335-380.

[121] Nelle versioni italiane viene impiegato il medesimo termine, "portabilità", in entrambi i regolamenti.

[122] L. Miglietti, *op. cit.*, pp. 8-13.

[123] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 18-21.

[124] *Ibidem*.

[125] Il rapporto giuridico sussistente tra utente professionale e fornitore del servizio non sempre può essere declinato all'interno della dinamica titolare-responsabile del trattamento come delineata dal GDPR, poiché l'assunzione di tali ruoli ha luogo solamente se sono coinvolti (anche) dati a carattere personale.

[126] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[127] J. Drexl, *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, Max Planck Institute for Innovation & Competition Research Paper No. 16-13, 2016, p. 55-66; T. Fia, *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in "Nuovo Notiziario Giuridico", 2019, n. 1, pp. 125-126; *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[128] M.L. Montagnani, *op. cit.*, pp. 304-310; *Parere del CESE sulla "Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"* - 2018/C 227/12, cit., pp. 5-6. In particolare: «In questo senso, il CESE ritiene che il regolamento all'esame dovrebbe almeno fornire un insieme di norme di base relative ai rapporti contrattuali tra i fornitori di servizi e gli utenti e prevedere una lista nera di clausole vietate a causa della limitazione del diritto di portabilità, secondo i parametri indicati in particolare nel suo parere sull'autoregolamentazione e sulla co-regolamentazione. Tuttavia, è inconcepibile che la Commissione non abbia neppure proposto di definire «orientamenti» per l'elaborazione dei codici di condotta precedentemente citati, come ha già fatto in altri settori, sostenuta in questo approccio dal CESE».

[129] Particolarmente azzeccata è l'osservazione secondo la quale è «anche dall'efficacia del Regolamento [sulla libera circolazione dei dati non personali] che si misura quella dell'intero quadro regolatorio sulla libera circolazione dei dati», in M.L. Montagnani, *op. cit.*, p. 304.

[130] Il termine "insiemi di dati misti", che compare in diversi documenti antecedenti all'approvazione del Regolamento, è stato poi ripreso dalla Commissione europea nelle Linee guida di maggio 2019.

[131] Riprendendo le parole della commissione, l'ipotesi dell'insieme indissolubilmente legato ricorre quando questo «contiene sia dati personali che dati non personali e separarli sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile», European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 10. Regolamento (UE) 2018/1807, art. 8.

[132] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 8-11.

[133] Regolamento (UE) 2018/1807, art. 8.

[134] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 8-11.

[135] G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in S. Sica, V. D'antonio, G.M.

Riccio, "La Nuova Disciplina Europea Sulla Privacy", Wolters Kluwer, 2016, pp. 55-78; A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in "Le Nuove Leggi Civili Commentate", 2017, 1, pp. 144-164.

[136] M. Finck, F. Pallas, *They who must not be identied – distinguishing personal from non-personal data under the GDPR*, in "International Data Privacy Law", 2020, n. 1, p. 11-36.

[137] A tal proposito, sia consentito rinviare a S. Torregiani, *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in "federalismi.it", 2020, n. 18, pp. 317-341.

[138] C. Flynn, *Shortcomings of the EU proposal for free flow of data*, in "InterMEDIA", 2018, n. 4, p. 30-35.

[139] Le difficoltà insite nell'identificazione del tipo di dato che si sta trattando non permettono sempre di raggiungere un risultato esatto in senso assoluto. In proposito, S. Forge, *op. cit.*, p. 1-6.

[140] M.L. Montagnani, *op. cit.*, pp. 304-310.

[141] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[142] *Ibidem.*

[143] Nonostante durante l'ultimo decennio si siano ritagliati uno spazio importante nell'ordinamento europeo, non è ancora chiaro quale natura giuridica debba essere riconosciuta ai codici di condotta. Le linee guida fornite dal Comitato europeo per la protezione dei dati definiscono i codici di condotta previsti dal GDPR, nello specifico all'articolo 40, come "strumenti di responsabilizzazione volontari" che possono rivelarsi utili "in quanto forniscono una descrizione dettagliata dei comportamenti più appropriati, in termini giuridici ed etici, con riguardo a un determinato settore" (così European Data Protection Board, Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679, 2019).

[144] J. Drexl, *op. cit.*

[145] M.L. Montagnani, *op. cit.*, pp. 311-313.

[146] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

* * *

The European legal framework for the free flow of data. The peril of a regulatory burden

Abstract: The increase in the free flow of data due to the digitalization has been followed by an even relevant growth of data localization restrictions required by EU member States legislative or administrative measures. The European legislator, willing to build a digital single market where all data can flow freely across EU, decided to face the data localization phenomenon through many different and sector-specific interventions, mainly based on the – still blurred – distinction between personal and non-personal data. Thanks to the analysis of the main sources of the European legal framework, this paper will assess if this patchwork, chosen over an overarching approach, is the most adequate for the common European data space.

Keywords: Free flow of data – Data localization – Personal data – Non-Personal Data