COMMISSIONE
EUROPEA

Bruxelles, 10.1.2017
COM(2017) 9 final

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"

{SWD(2017) 2 final}

"COSTRUIRE UN'ECONOMIA DEI DATI EUROPEA"

1. INTRODUZIONE

I dati sono diventati una risorsa essenziale per la crescita economica, la creazione di posti di lavoro e il progresso sociale. L'analisi dei dati facilita l'ottimizzazione di processi e decisioni, l'innovazione e la predizione di eventi futuri. È una tendenza mondiale che presenta potenzialità enormi in vari campi: sanità, sicurezza alimentare, clima, uso efficiente delle risorse, energia, sistemi di trasporto intelligenti e città intelligenti.

L'"economia dei dati"[1] è caratterizzata da un ecosistema di diversi tipi di operatori del mercato, quali produttori, ricercatori e fornitori di infrastrutture, che collaborano fra loro per rendere i dati accessibili e utilizzabili. Ciò consente agli operatori del mercato di estrarre valore dai dati, creando una varietà di applicazioni con un notevole potenziale di migliorare la vita quotidiana (ad esempio gestione del traffico, ottimizzazione dei raccolti e assistenza sanitaria a distanza).

Il valore dell'economia dei dati nell'UE è stato stimato a 257 miliardi di euro nel 2014, pari all'1,85% del PIL dell'UE[2], passati a 272 miliardi di euro nel 2015, ossia all'1,87% del PIL dell'UE (per un incremento annuo del 5,6%). La stessa stima prevede che, istituendo per tempo un assetto programmatico e giuridico per l'economia dei dati, il suo valore potrà raggiungere i 643 miliardi di euro nel 2020, pari al 3,17% del PIL complessivo dell'UE.

A norma del regolamento generale sulla protezione dei dati (RGPD)[3], a partire dal maggio 2018 un unico insieme paneuropeo di norme sostituirà le attuali 28 normative nazionali. Grazie al nuovo meccanismo di sportello unico[4], un'unica autorità per la protezione dei dati (APD) sarà responsabile del controllo delle attività di trattamento dei dati svolte a livello transfrontaliero da un'impresa nell'UE. Sarà garantita la coerenza nell'interpretazione delle nuove norme. In particolare, nei casi transfrontalieri in cui sono coinvolte diverse APD nazionali, si adotterà una decisione unica per assicurare che problemi comuni ricevano soluzioni comuni. Inoltre, il regolamento generale sulla protezione dei dati istituisce condizioni di parità fra le imprese europee e straniere,

---

1 L'economia dei dati misura l'impatto complessivo del mercato dei dati — vale a dire il mercato in cui i dati digitali sono scambiati in forma di prodotti o servizi derivati dai dati grezzi — sull'economia nel suo insieme. Comprende la produzione, la raccolta, la conservazione, il trattamento, la distribuzione, l'analisi, l'elaborazione, la consegna e l'utilizzo dei dati ottenuti mediante tecnologie digitali (European Data Market study, SMART 2013/0063, IDC, 2016).

2 European Data Market study, SMART 2013/0063, IDC, 2016.

3 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 95/56/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

4 Articolo 56 del regolamento generale sulla protezione dei dati.

imponendo alle imprese che hanno sede fuori dell'UE di applicare le stesse regole cui sono tenute le imprese europee se offrono beni e servizi o monitorano il comportamento di persone nell'UE. Un maggiore livello di fiducia dei consumatori andrà a beneficio sia dell'UE, sia degli operatori commerciali esterni.

La direttiva e-Privacy disciplina la riservatezza dei servizi di comunicazione elettronica nell'Unione europea. Sarà sostituita da un regolamento[5], proposto in parallelo alla presente comunicazione, che ha lo scopo di garantire un livello elevato di protezione in piena coerenza con il regolamento generale sulla protezione dei dati. Una normativa rigorosa sulla protezione dei dati crea il clima di fiducia necessario per lo sviluppo dell'economia digitale in tutti i settori del mercato interno.

Come ha sottolineato il presidente Juncker nel suo discorso sullo stato dell'Unione del 14 settembre 2016, "*[e]ssere europei significa avere diritto alla protezione dei propri dati personali mediante rigorose leggi europee. Perché agli europei non piace essere sorvolati da droni che registrano ogni loro movimento, né vogliono che le imprese tengano traccia di ogni loro click in rete. Per questa ragione, nel maggio di quest'anno, il Parlamento, il Consiglio e la Commissione hanno concordato un regolamento sulla protezione comune europea dei dati. Si tratta di una rigorosa normativa europea sul trattamento dei dati personali che si applica alle imprese, ovunque abbiano sede. Perché in Europa ci teniamo alla riservatezza. Si tratta di una questione di dignità umana.*"

Nella comunicazione del 2012 dal titolo "Salvaguardare la privacy in un mondo interconnesso — Un quadro europeo della protezione dei dati per il XXI secolo"[6] e in quella del 2014 dal titolo "Verso una florida economia basata sui dati"[7], la Commissione ha riconosciuto che occorrono norme moderne e coerenti valide in tutta l'UE per consentire ai dati di circolare liberamente da uno Stato membro all'altro e che l'economia digitale europea è stata troppo lenta nell'abbracciare la rivoluzione dei dati rispetto a quella degli Stati Uniti e non dispone di una capacità industriale equivalente. La Commissione ha concluso che la mancanza di un contesto giuridico adatto agli scambi di dati nell'UE può limitare l'accesso ai grandi insiemi di dati, eventualmente ostacolare l'ingresso di nuovi operatori sul mercato e frenare l'innovazione.

Restrizioni ingiustificate **alla libera circolazione dei dati** potrebbero frenare lo sviluppo dell'economia dei dati nell'UE. Tali restrizioni riguardano i requisiti imposti dalle autorità pubbliche in materia di ubicazione dei dati per la conservazione o l'elaborazione. La questione della libera circolazione dei dati riguarda tutti i tipi di dati: imprese e soggetti attivi nell'economia dei dati hanno a che fare con dati industriali e generati automaticamente, personali e non, e con dati creati con l'intervento dell'uomo. Nella strategia per il mercato unico digitale la Commissione ha annunciato che proporrà un'iniziativa per affrontare il problema delle limitazioni alla libera circolazione dei dati all'interno dell'UE in ambiti diversi dalla protezione dei dati personali e delle limitazioni ingiustificate collegate all'ubicazione dei dati per la conservazione o l'elaborazione. Tali restrizioni comprendono atti giuridici adottati dagli Stati membri e norme e prassi amministrative aventi il medesimo effetto. Il loro numero tende ad aumentare con

[5] COM(2017) 10 final.

[6] COM(2012) 9 final.

[7] COM(2014) 442 final.

l'espansione dell'economia dei dati, generando così incertezza su dove i dati possano essere conservati o elaborati. Ne può derivare un impatto in tutti i settori dell'economia e in organizzazioni del settore sia pubblico sia privato, che potrebbero avere difficoltà ad accedere a servizi di dati innovativi e/o più economici. Restrizioni ingiustificate in materia di ubicazione dei dati compromettono la libera prestazione dei servizi e la libertà di stabilimento, sancite dal trattato, e violano il diritto derivato vigente. Si rischia così di frammentare il mercato, riducendo la qualità del servizio per gli utenti e la competitività dei fornitori di servizi, soprattutto i più piccoli.

Anche le localizzazioni di dati non giustificate fanno parte delle discussioni tra l'UE e i suoi partner commerciali, tenuto conto dell'importanza crescente dei dati e dei servizi di dati nell'economia globale e dei potenziali atteggiamenti dei paesi terzi al riguardo. Le norme dell'UE di protezione dei dati non sono negoziabili in sede di accordo di libero scambio. Come spiegato nella comunicazione della Commissione sullo scambio e la protezione dei dati personali in un mondo globalizzato[8], il dialogo sulla protezione dei dati e i negoziati commerciali con i paesi terzi devono procedere su binari diversi. Oltre a ciò, come indicato nella comunicazione Commercio per tutti[9], la Commissione cercherà di approfittare degli accordi commerciali dell'UE per stabilire una disciplina del commercio elettronico e dei flussi transfrontalieri di dati e affrontare nuove forme di protezionismo digitale, rispettando e preservando pienamente le norme sulla protezione dei dati dell'UE.

Inoltre, con la sempre maggiore penetrazione delle trasformazioni basate sui dati nell'economia e nella società, crescenti quantità di dati sono generate da macchine o processi supportati da tecnologie emergenti, quali l'internet delle cose (IoT), le fabbriche del futuro e i sistemi autonomi connessi. La connettività stessa cambia il modo in cui i dati sono accessibili: dati che prima erano accessibili mediante collegamenti fisici oggi sono disponibili a distanza. Iniziano solo ora ad emergere sia l'enorme diversità delle fonti e dei tipi di dati, sia la ricchezza di possibilità di sfruttamento di quei dati in tutta una serie di settori, anche per l'elaborazione di politiche pubbliche. Per trarre vantaggio da tali opportunità, i soggetti attivi pubblici e privati del mercato dei dati devono poter accedere a insiemi di dati vasti e diversificati. Le questioni dell'accesso e della trasmissione in relazione ai dati generati dalle macchine o dai processi sono dunque al centro dell'emergere di un'economia basata sui dati e richiedono un'attenta valutazione.

Altre questioni emergenti riguardano l'applicazione delle norme sulla responsabilità ai danni causati da un difetto di un dispositivo o di un robot connesso e la portabilità e l'interoperabilità dei dati. Nel contesto di nuove tecnologie quali l'internet delle cose (IoT) e la robotica, esistono interdipendenze complesse e sofisticate sia all'interno dei prodotti stessi (hardware e software) sia fra dispositivi interconnessi. Nuove questioni possono inoltre presentarsi nel contesto delle macchine autonome, che potrebbero avere comportamenti imprevisti e indesiderati tali da causare danni alle persone e alle cose. Questi fenomeni possono creare incertezza giuridica relativamente all'applicazione del quadro normativo esistente in materia di responsabilità e sicurezza.

---

8 COM(2017) 7 final.

9 COM(2015) 497 final.

Come annunciato nella strategia per il mercato unico digitale, la Commissione mira a creare un quadro programmatico e giuridico chiaro e specifico per l'economia dei dati, eliminando gli ostacoli rimanenti alla circolazione dei dati e affrontando le incertezze giuridiche create dalle nuove tecnologie dei dati. Altri obiettivi cui ambisce la presente comunicazione sono l'aumento della disponibilità e dell'utilizzo dei dati, la promozione di nuovi modelli di impresa nel settore dei dati, il miglioramento delle condizioni di accesso ai dati e lo sviluppo dell'analisi dei dati nell'UE. A tal fine, la Commissione ha individuato temi di discussione specifici volti a "costruire un'economia dei dati europea".

La presente comunicazione esamina pertanto le questioni seguenti: libero flusso dei dati; accesso e trasferimento per i dati generati da macchine; responsabilità e sicurezza nel contesto delle tecnologie emergenti; portabilità dei dati non personali, interoperabilità e norme. La presente comunicazione contiene inoltre proposte per la sperimentazione di soluzioni normative comuni in ambiente reale.

La Commissione sta avviando un ampio dialogo con le parti interessate in merito alle questioni esaminate nella presente comunicazione. Primo passo di questo dialogo è una consultazione pubblica, avviata in parallelo al pacchetto per l'economia dei dati[10].

2. LIBERO FLUSSO DEI DATI

Un'economia dei dati funzionante e dinamica richiede che il flusso di dati nel mercato interno sia effettivo e tutelato. In un contesto tecnologico in rapida evoluzione, un libero flusso di dati sicuro e affidabile è essenziale per tutelare le quattro libertà fondamentali del mercato unico dell'UE sancite dai trattati (merci, lavoratori, servizi e capitali). I servizi di dati sono in rapida crescita nell'Unione europea e nel mondo. Un mercato unico efficiente e senza barriere in questo settore creerebbe opportunità significative per la crescita e l'occupazione.

La crescita e l'innovazione nell'economia dei dati e l'attuazione di servizi pubblici transfrontalieri possono essere compromesse da barriere alla libera circolazione dei dati nell'UE, quali ingiustificati requisiti di localizzazione dei dati imposti dalle autorità pubbliche. Misure di localizzazione dei dati rappresentano di fatto la reintroduzione di "controlli di frontiera" digitali[11]. Spaziano da esigenze delle autorità di vigilanza che impongono ai fornitori di servizi finanziari di conservare i loro dati in loco, all'attuazione di norme sul segreto professionale che prescrivono la conservazione o l'elaborazione dei dati a livello locale, a normative che prescrivono l'immagazzinamento locale di informazioni archiviate generate dal settore pubblico, indipendentemente dalla loro sensibilità.

Le preoccupazioni relative alla privacy sono legittime, ma non devono essere utilizzate dalle amministrazioni pubbliche come motivo per limitare il libero flusso dei dati in modo ingiustificato. Come sopra indicato, il regolamento generale sulla protezione dei dati prevede un unico insieme di norme per un livello elevato di protezione dei dati personali in tutta l'UE. Rafforza la fiducia dei consumatori nei servizi online e assicura

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

[11] OCSE, "Emerging Policy Issues: Localisation Barriers to Trade", 2015 e lavori in preparazione.

un'applicazione uniforme delle norme in tutti gli Stati membri, mediante il potenziamento delle autorità nazionali per la protezione dei dati. Il regolamento promuove la fiducia necessaria al trattamento dei dati e costituisce la base per la libera circolazione dei dati personali nell'UE. Vieta le restrizioni alla libera circolazione dei dati personali all'interno dell'Unione allorché si fondano su motivi connessi alla protezione dei dati personali[12]. Tuttavia, restrizioni fondate su motivi diversi dalla protezione dei dati personali, ad esempio nell'ambito della normativa fiscale o contabile, non rientrano nel campo di applicazione del regolamento. Inoltre, i dati non personali, cioè quelli che non si riferiscono a una persona fisica identificata o identificabile[13], rimangono al di fuori del campo di applicazione del regolamento e possono riguardare, ad esempio, i dati non personali generati da macchine.

Le restrizioni in materia di ubicazione dei dati possono derivare da disposizioni di legge o da orientamenti amministrativi o pratiche che richiedono la conservazione o l'elaborazione dei dati[14] in un formato elettronico[15] limitato ad una determinata zona geografica o giurisdizione. A volte le restrizioni sono imposte dagli Stati membri nella convinzione che le autorità di vigilanza possano controllare più facilmente i dati immagazzinati localmente. La localizzazione è anche utilizzata come surrogato di garanzie in termini di riservatezza, audit, controllo dell'osservanza e sicurezza dei dati. In pratica, tuttavia, raramente queste misure contribuiscono agli obiettivi che intendono raggiungere.

La sicurezza delle informazioni dipende anche da una serie di altri fattori, oltre che dall'ubicazione fisica in cui sono conservati i dati, fra cui la preservazione della loro riservatezza e integrità nel momento in cui diventano disponibili al di fuori della struttura di conservazione. Veri fautori di sicurezza nella conservazione e nell'elaborazione dei dati non sono le restrizioni all'ubicazione dei dati, bensì le migliori pratiche della gestione informatica di ultima generazione applicate su scala molto maggiore di quella dei sistemi individuali. Ad esempio, per conservare i dati al sicuro da disastri naturali o attacchi informatici che colpiscono una determinata località, le strutture di conservazione dei dati ubicate in diversi Stati membri possono fungere da backup le une per le altre e avvalersi delle misure tecniche e organizzative previste dalla direttiva sulla sicurezza delle reti e dei sistemi d'informazione[16]. Inoltre, la disponibilità di dati per scopi di regolamentazione o di vigilanza, che non si vuole in alcun modo mettere in questione, potrebbe realizzarsi meglio rafforzando la cooperazione tra le autorità nazionali o fra tali autorità e il settore privato, anziché mediante restrizioni di localizzazione. In effetti, in un settore caratterizzato da una stretta cooperazione tra le autorità di controllo, come ad

---

12 Articolo 1, paragrafo 3. Ad esempio, un indirizzo IP dinamico, registrato da un fornitore di servizi audiovisivi online all'accesso di una persona a un sito web, che il fornitore rende pubblicamente accessibile costituisce un dato personale, relativamente a tale fornitore, in quanto quest'ultimo ha i mezzi giuridici che gli consentono di identificare l'interessato in congiunto con altri dati detenuti dal fornitore di servizi Internet riguardanti tale persona. Cfr. la sentenza nella causa C-582/14, Breyer, ECLI:EU:C:2016:779, punto 49.

13 Ai sensi dell'articolo 4, paragrafo 1, del regolamento generale sulla protezione dei dati.

14 Dati detenuti sia da privati sia dal settore pubblico.

15 Comprese copie di insiemi di dati.

16 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

esempio quello dei servizi finanziari, i requisiti di localizzazione dei dati potrebbero rivelarsi controproducenti[17].

Ciò nonostante, requisiti di localizzazione dei dati possono essere giustificati e proporzionati in specifici contesti o relativamente a certi dati, in particolare prima che sia predisposta un'efficace cooperazione transfrontaliera, ad esempio per assicurare il trattamento sicuro di dati relativi a infrastrutture critiche dell'energia o la disponibilità di prove elettroniche (in forma, ad esempio, di copie di insieme di dati localizzati) ad uso delle autorità giudiziarie, oppure l'immagazzinamento locale dei dati in determinati registri pubblici.

Purtroppo, sia a livello globale sia in Europa esiste una tendenza verso una maggiore localizzazione dei dati, che spesso scaturisce dall'errore di ritenere che i servizi localizzati siano automaticamente più sicuri di quelli transfrontalieri. Inoltre, il mercato dei servizi di dati è molto influenzato dall'assenza di norme trasparenti e dalla forte percezione della necessità di localizzare i dati. Ciò può limitare l'accesso delle imprese e delle organizzazioni del settore pubblico a servizi di dati più economici o più innovativi o costringere le imprese che operano a livello transfrontaliero a predisporre capacità in eccesso di conservazione e trattamento dei dati. Questa situazione potrebbe anche dissuadere imprese incentrate sui dati, in particolare nuove imprese e PMI, dall'intensificare le loro attività, dall'entrare in nuovi mercati (ad esempio di fronte all'obbligo di creare centri dati in 28 Stati membri) o dal centralizzare le capacità di trattamento e analisi dei dati al fine di sviluppare nuovi prodotti e servizi.

Attualmente l'Europa deriva l'84% della propria domanda finale di "servizi informatici" (consultazione, hosting, sviluppo) dall'interno dell'Unione europea. Se anche tali servizi potessero operare più facilmente all'interno dell'UE grazie alla rimozione delle restrizioni di localizzazione dei dati, potrebbero derivarne fino a 8 miliardi di euro all'anno di aumento del PIL in guadagni di costo e di efficienza[18].

La localizzazione dei dati ostacola anche una più ampia adozione del cloud storage e del cloud computing, con possibili ripercussioni più ampie anche a livello sociale. In effetti, un uso più efficiente delle risorse informatiche potrebbe contribuire a ridurre il consumo netto di energia e le emissioni nette di CO_2 del 30% o più. Una piccola impresa che si trasferisce nel cloud potrebbe ridurre il proprio consumo di energia e le proprie emissioni di CO_2 di più del 90%, facendo funzionare le sue applicazioni aziendali nella nuvola anziché su infrastruttura propria. Si prevede che il mercato mondiale dei centri di dati efficienti sotto il profilo energetico aumenti fino a rappresentare un valore di quasi 90 miliardi di EUR entro fine 2020. La frammentazione del mercato dei servizi di dati ostacolerebbe il pieno sviluppo nell'UE di questi servizi più efficienti sotto il profilo energetico e metterebbe a rischio la disponibilità a investire.

---

[17] Numerose disposizioni UE sui servizi finanziari e sul sistema europeo di vigilanza finanziaria prescrivono che le autorità di vigilanza abbiano accesso ai dati sulle operazioni e sugli istituti finanziari in tutto il territorio dell'UE. Il fatto di richiedere che i dati siano conservati in un determinato territorio nazionale o di subordinarne l'accesso all'espletamento di procedure amministrative potrebbe ridurre l'accesso delle autorità di vigilanza a dati essenziali per l'esecuzione del loro mandato.

[18] "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", ECIPE 2016, calcolo basato sull'aumento della pressione concorrenziale nell'ambito di un mercato unico digitale "industriale" con piena trasparenza dei prezzi.

Per affrontare le questioni e le restrizioni sopra descritte e realizzare pienamente il potenziale dell'economia europea dei dati, è necessario che le azioni degli Stati membri che riguardano la conservazione e l'elaborazione dei dati seguano un "**principio della libera circolazione dei dati all'interno dell'UE**", a complemento degli obblighi di libera circolazione dei servizi e delle disposizioni sulla libertà di stabilimento sanciti dal trattato e dal relativo diritto derivato. Restrizioni sull'ubicazione dei dati già esistenti o nuove dovrebbero essere rigorosamente motivate alla luce del trattato e del relativo diritto derivato per verificare se siano necessarie e proporzionate al raggiungimento di un obiettivo imperativo di interesse generale, quale ad esempio la pubblica sicurezza[19].

Il principio della libera circolazione dei dati personali[20], sancito dal diritto primario e secondario, dovrebbe valere anche nei casi in cui il regolamento generale sulla protezione dei dati consente agli Stati membri di disciplinare materie specifiche. Gli Stati membri dovrebbero essere incoraggiati a non fare uso delle clausole di deroga del regolamento per limitare ulteriormente la libera circolazione dei dati.

Nelle sue conclusioni del 15 dicembre 2016, il Consiglio europeo ha invitato a eliminare gli ostacoli che ancora restano all'interno del mercato unico, fra cui quelli che impediscono la libera circolazione dei dati[21].

Per applicare il principio della libera circolazione dei dati, la Commissione si muoverà in due fasi.

- A seguito della pubblicazione della presente comunicazione, la Commissione intende avviare un dialogo strutturato con gli Stati membri e altre parti interessate riguardo alla motivazione e alla proporzionalità delle misure in materia di ubicazione dei dati, prendendo come punto di partenza le restrizioni finora individuate dalla Commissione.

- A seguito dei risultati dei dialoghi e in base a ulteriori elementi raccolti sulla portata e sulla natura delle restrizioni in materia di ubicazione dei dati e sui loro impatti, in particolare sulle PMI e sulle start-up, anche mediante la consultazione pubblica annessa, la Commissione potrà, se necessario, avviare procedimenti di infrazione nei confronti di misure ingiustificate o sproporzionate in materia di ubicazione dei dati e, se del caso, adottare ulteriori iniziative sul libero flusso dei dati. In tale contesto, eventuali ulteriori interventi saranno realizzati in conformità ai principi di migliore regolamentazione.

[19] Tenendo conto del fatto che le eccezioni al trattato vanno interpretate in modo restrittivo. Gli atti di diritto derivato pertinenti comprendono il regolamento generale sulla protezione dei dati, la direttiva 2000/31/CE (direttiva sul commercio elettronico), la direttiva 2006/123/CE (direttiva "servizi") e, per quanto riguarda i progetti di norme tecniche e di norme in materia di servizi della società dell'informazione, la direttiva 2015/1535 (direttiva sulla trasparenza).

[20] La libera circolazione dei dati personali è sancita dall'articolo 16 del trattato sul funzionamento dell'Unione europea e le norme sulla libera circolazione dei dati personali figurano nella normativa attuale e futura dell'UE in materia di protezione dei dati. L'articolo 1, paragrafo 3, del regolamento generale sulla protezione dei dati recita: "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".

[21] http://www.consilium.europa.eu/it/press/press-releases/2016/12/15-euco-conclusions-final/

3. ACCESSO AI DATI E TRASFERIMENTO DI DATI

Quantità sempre maggiori di dati sono generati da macchine o da processi basati su tecnologie emergenti, come la cosiddetta "internet delle cose". Tali dati sono utilizzati sempre più di frequente come componente essenziale di servizi nuovi e innovativi, per migliorare prodotti o processi produttivi e dare sostegno al processo decisionale.

La diversità dei dati generati da queste macchine o processi offre ampie opportunità agli operatori del mercato dei dati di innovare e sfruttare tali dati. Ad esempio, i dati rilevati dai sensori usati nelle aziende agricole moderne potrebbero servire a creare un'applicazione per ottimizzare il raccolto e i dati generati da sensori installati ai semafori potrebbero servire a creare un'applicazione di gestione del traffico o di ottimizzazione dei percorsi.

Per ottenere il massimo valore da questo tipo di dati, gli operatori del mercato hanno bisogno di accedere a insiemi di dati ampi e diversificati. Tuttavia, ciò risulta difficile se i generatori dei dati li tengono per sé e i dati sono poi analizzati in compartimenti stagni. Le questioni dell'accesso e del trasferimento in relazione ai dati grezzi (cioè non trattati o modificati dopo la raccolta) generati dalle macchine o dai processi sono dunque al centro dell'emergere di un'economia basata sui dati e richiedono un'attenta valutazione.

La questione dell'accesso ai dati generati da macchine è di attualità in diversi settori, quali i trasporti, i mercati dell'energia, la domotica e i settori sanitario e assistenziale.

Prima di esaminare l'attuale situazione dell'accesso ai dati nell'UE, è importante chiarire il tipo dei dati considerati nel presente contesto.

3.1. Tipo dei dati considerati

In generale, i dati possono essere personali o non personali. Ad esempio, i dati generati da sensori di temperatura domestici possono essere di natura personale se riferiti a una persona vivente, mentre quelli sull'umidità del suolo sono non personali. I dati personali possono essere trasformati in dati non personali mediante anonimizzazione. Se i dati rientrano nella categoria dei dati personali[22], si applica il quadro per la protezione dei dati, in particolare il regolamento generale sulla protezione dei dati.

I dati generati da macchine sono prodotti da processi, applicazioni o servizi informatici, senza intervento umano diretto, oppure da sensori che trattano informazioni provenienti da apparecchiature, software o macchine, virtuali o reali.

I dati generati da macchine possono essere personali o non personali. Sono personali se consentono l'identificazione di una persona fisica e in tal caso sono soggetti a tutte le norme sui dati personali fino a quando non siano pienamente anonimizzati (come, ad esempio, i dati di localizzazione delle applicazioni mobili).

Un filo comune fra il tema del libero flusso dei dati e le nuove problematiche di accesso e trasmissione dei dati sta nel fatto che le imprese e i soggetti dell'economia dei dati tratteranno dati sia personali sia non personali e che i flussi e gli insiemi di dati

[22] Ai sensi dell'articolo 4, paragrafo 1, del regolamento generale sulla protezione dei dati.

conterranno abitualmente entrambi i tipi. Le misure programmatiche devono tenere conto di questa realtà economica e del quadro giuridico sulla protezione dei dati personali, nel rispetto dei diritti fondamentali degli individui.

3.2. Limiti all'accesso ai dati

Per valutare tale problematica emergente, è necessario in primo luogo analizzare il modo in cui le imprese e altri operatori del mercato hanno accesso ai vasti e diversificati insiemi di dati necessari per l'economia dei dati.

Gli elementi acquisiti[23] indicano che le società titolari di grandi quantità di dati tendono in generale ad analizzare i dati al proprio interno. Nella maggior parte dei casi i dati sono generati e analizzati dalla stessa impresa e anche in caso di subappalto della funzione di analisi il riutilizzo dei dati può essere escluso. Inoltre, in alcuni casi, fabbricanti, imprese di servizi e altri operatori del mercato in possesso di dati tengono per sé i dati generati dalle loro macchine o mediante i loro prodotti e servizi, contribuendo così, potenzialmente, a limitarne il riutilizzo nei mercati a valle. Molte imprese non dispongono di interfacce di programmazione delle applicazioni (API)[24] facili da usare o non le annoverano fra le opzioni possibili (sono interfacce che specificano come le diverse applicazioni debbano interagire le une con le altre), nonostante possano servire da punti di accesso sicuro per usi nuovi e innovativi dei dati detenuti dalle imprese.

Nel complesso, pertanto, lo scambio di dati resta attualmente limitato. I mercati di dati stanno lentamente emergendo, ma non sono ampiamente utilizzati. Le imprese possono non avere strumenti e competenze adeguati per quantificare il valore economico dei dati in loro possesso e possono temere di perdere o compromettere il proprio vantaggio competitivo rendendoli disponibili ai concorrenti.

3.3. Dati grezzi generati da macchine: situazione giuridica ai livelli dell'UE e nazionale

I dati grezzi generati da macchine non sono protetti da diritti di proprietà intellettuale esistenti, perché non sono considerati il risultato di un impegno intellettuale e/o dotati di un grado di originalità. Il diritto *sui generis* della direttiva sulle banche dati (96/9/CE) — che conferisce al costitutore della banca dati il diritto di vietare l'estrazione e/o il reimpiego della totalità o di una parte sostanziale del suo contenuto — può offrire protezione solo a condizione che la creazione della banca dati comporti un investimento rilevante collegato al conseguimento, alla verifica o alla presentazione del contenuto di quest'ultima. La direttiva sulla protezione del segreto commerciale (2016/943/UE), di recente adozione, da recepire nel diritto nazionale entro giugno 2018, garantirà la protezione del segreto commerciale contro l'acquisizione, l'utilizzo e la divulgazione. Affinché i dati godano della qualifica di "segreto commerciale", occorre adottare misure

[23] IDC, European Data Market Study, Prima relazione intermedia, 2016; Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, Prima relazione intermedia, 2016; Conferenza ad alto livello, DG Connect, 17 ottobre 2016.

[24] Ad esempio: https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

per salvaguardare la segretezza delle informazioni, che rappresentano un "capitale intellettuale dell'impresa".

In base alla normativa vigente in diversi Stati membri, esiste un diritto riferito ai dati solo quando questi soddisfano determinate condizioni per godere, ad esempio, di un diritto di proprietà intellettuale, di un diritto sulle banche dati o di una qualifica di segreto commerciale. Tuttavia, a livello di UE i dati grezzi generati da macchine in quanto tali di norma non soddisfano tali condizioni.

Non esistono dunque, allo stato attuale, quadri programmatici complessivi a livello nazionale o dell'Unione in relazione ai dati grezzi generati da macchine non classificabili come dati personali o alle condizioni del loro sfruttamento economico e commerciabilità. La questione risulta così in gran parte affidata a soluzioni contrattuali. L'uso del diritto contrattuale vigente e di strumenti del diritto della concorrenza disponibili nell'Unione potrebbe essere una risposta adeguata. Si potrebbe anche ipotizzare il ricorso ad accordi volontari o ad accordi quadro in alcuni settori. Tuttavia, nei casi in cui il potere negoziale dei diversi operatori del mercato è diseguale, le soluzioni basate sul mercato potrebbero rivelarsi insufficienti, da sole, a garantire risultati equi e favorevoli all'innovazione, ad agevolare l'accesso di nuovi operatori del mercato e a evitare effetti di *lock-in*.

3.4. Situazione di fatto

In alcuni casi i fabbricanti o i fornitori di servizi possono diventare di fatto "proprietari" dei dati generati dalle loro macchine o processi, anche quando i dispositivi stessi sono di proprietà dell'utilizzatore. Un controllo *de facto* dei dati può essere fonte di differenziazione e di vantaggio competitivo per i fabbricanti. Può però rivelarsi problematico perché spesso il fabbricante vieta all'utilizzatore di autorizzare l'uso dei dati a un altro soggetto.

In tal modo, i diversi operatori del mercato che controllano i dati possono, a seconda delle specificità dei mercati, trarre vantaggio dalle lacune del quadro normativo o dalle incertezze giuridiche sopra descritte, imponendo agli utilizzatori clausole vessatorie o mediante mezzi tecnici quali formati proprietari o cifratura. Numerosi Stati membri - ma non tutti - hanno esteso il campo di applicazione della direttiva sulla tutela dei consumatori in materia di clausole contrattuali abusive anche alle transazioni B2B. Una conseguenza potrebbe essere, ad esempio, l'assoggettamento di determinati utilizzatori e imprese a modalità esclusive di sfruttamento dei dati. Potrebbero emergere accordi volontari di condivisione dei dati, ma la negoziazione dei relativi contratti potrebbe comportare costi di transazione significativi per la parte più debole in caso di posizione negoziale disuguale o di costi elevati dei servizi di consulenza giuridica.

3.5. Un futuro quadro dell'UE per l'accesso ai dati

Attualmente alcuni Stati membri stanno esplorando la possibilità di assicurare l'accesso ai dati generati da macchine e potrebbero decidere di regolamentare la questione autonomamente. Un approccio non coordinato rischierebbe di creare frammentazione e sarebbe dannoso per lo sviluppo dell'economia dell'UE e il funzionamento transfrontaliero dei servizi e delle tecnologie dei dati nel mercato interno.

Di conseguenza, la Commissione intende avviare un dialogo con gli Stati membri e le altre parti interessate al fine di esplorare la possibilità di un futuro quadro dell'UE per l'accesso ai dati. A parere della Commissione, tale dialogo dovrebbe articolarsi sulle modalità più efficaci per conseguire gli obiettivi seguenti.

- **Migliorare l'accesso ai dati anonimi generati da macchine**: mediante la condivisione, il riutilizzo e l'aggregazione, i dati generati da macchine diventano una fonte di creazione di valore, innovazione e diversità dei modelli commerciali[25].

- **Facilitare e incentivare la condivisione dei dati**: future soluzioni dovrebbero promuovere un accesso effettivo ai dati, tenendo conto, ad esempio, di eventuali differenze di potere contrattuale tra operatori del mercato.

- **Tutelare gli investimenti e i patrimoni acquisiti**: future soluzioni dovrebbero anche tenere conto degli interessi legittimi degli operatori del mercato che investono nello sviluppo dei prodotti, garantire un equo ritorno sui loro investimenti e contribuire in tal modo all'innovazione. Al contempo, tali soluzioni dovrebbero assicurare una ripartizione equa dei benefici tra i titolari dei dati[26], gli addetti al trattamento e i fornitori di applicazioni, nell'ambito delle catene del valore.

- **Evitare la divulgazione di dati riservati**: future soluzioni dovrebbero ridurre i rischi di divulgazione di dati riservati, in particolare ai concorrenti attuali o potenziali. Al riguardo, occorrerebbe anche disporre un'adeguata classificazione dei dati prima di valutare se un determinato componente possa essere condiviso.

- **Ridurre al minimo gli effetti di *lock-in***: si dovrebbe tenere conto delle disparità di potere contrattuale fra imprese e soggetti privati. Occorre evitare effetti di *lock-in*, in particolare per le PMI, le start-up e i privati.

Nei dialoghi con le parti interessate, la Commissione intende discutere le seguenti possibilità per affrontare la questione dell'accesso ai dati generati da macchine, che presentano diversi livelli di intervento.

- **Orientamenti per incentivare le imprese a condividere i dati**: per attenuare gli effetti di normative nazionali divergenti e offrire una maggiore certezza del diritto alle imprese, la Commissione potrebbe pubblicare orientamenti su come contemplare nei contratti i diritti di controllo sui dati non personali. Tali orientamenti si baserebbero sulla legislazione vigente, segnatamente i requisiti di trasparenza ed equità stabiliti dalle normative dell'UE in materia di commercio e tutela dei consumatori, la direttiva sul segreto commerciale e la normativa sui diritti d'autore, con particolare riguardo alla direttiva sulle banche dati. La Commissione intende avviare nel 2017 una valutazione della direttiva sulle banche dati.

[25] Ai dati personali si applica il regolamento generale sulla protezione dei dati.

[26] Il soggetto che gestisce e conserva nella pratica i dati generati da macchine.

- **Promuovere lo sviluppo di soluzioni tecniche affidabili di identificazione e scambio di dati**: la tracciabilità e l'individuazione chiara delle fonti dei dati sono una condizione preliminare per un reale controllo dei dati nel mercato. Per creare un clima di fiducia nel sistema può essere necessario definire protocolli affidabili ed eventualmente standardizzati di identificazione persistente delle fonti dei dati. Anche le interfacce di programmazione delle applicazioni (API) possono stimolare la creazione di un ecosistema per ideatori di applicazioni e algoritmi interessati ai dati detenuti dalle imprese. Le API possono aiutare le imprese e le autorità pubbliche a individuare e sfruttare diversi tipi di riutilizzo dei dati in loro possesso. Su tale base, si potrebbe prendere in considerazione un uso più ampio di API aperte, standardizzate e ben documentate, mediante orientamenti tecnici che comprendano l'identificazione e la diffusione delle migliori pratiche per le imprese e gli enti pubblici. Ciò potrebbe comprendere la messa a disposizione di dati in formati adatti alla lettura ottica e la fornitura dei relativi metadati.

- **Norme contrattuali minime**: norme minime potrebbero prevedere una soluzione equilibrata di riferimento per i contratti sui dati, tenendo debitamente conto anche del controllo di idoneità in corso sul funzionamento globale della direttiva sulle clausole contrattuali abusive. Vi si potrebbe aggiungere l'introduzione di controlli di iniquità nei rapporti contrattuali B2B[27] che consentano di invalidare le clausole contrattuali che si discostano eccessivamente dalle norme predefinite. Potrebbero inoltre essere integrate da un insieme di clausole contrattuali standard raccomandate, elaborate a cura delle parti interessate. Questo approccio potrebbe ridurre gli ostacoli di natura giuridica per le piccole imprese e attenuare lo squilibrio fra posizioni negoziali, pur mantenendo un ampio grado di libertà contrattuale.

- **Accesso per fini scientifici e di interesse pubblico**: si potrebbe concedere l'accesso ai dati alle autorità pubbliche qualora fosse nell'"interesse generale" e potesse migliorare considerevolmente il funzionamento del settore pubblico, come ad esempio l'accesso degli uffici di statistica ai dati commerciali o l'ottimizzazione dei sistemi di gestione del traffico sulla base di dati in tempo reale inviati da veicoli privati. L'accesso ai dati commerciali da parte delle autorità statistiche in linea di massima contribuirebbe ad alleviare gli oneri di informativa che gravano sugli operatori economici. Analogamente, l'accesso ai dati e la capacità di combinare quelli provenienti da fonti diverse è fondamentale per la ricerca scientifica in settori quali la medicina e le scienze sociali e ambientali.

- **Diritti dei produttori di dati**: il diritto di utilizzare e di autorizzare l'utilizzo di dati non personali potrebbe essere conferito al "produttore dei dati", vale a dire il proprietario o l'utilizzatore a lungo termine (locatario) del dispositivo. Tale approccio mirerebbe a chiarire la situazione giuridica e a offrire una scelta più ampia al produttore di dati, rendendo possibile agli utilizzatori l'utilizzo dei loro dati e contribuendo così a sbloccare i dati generati da macchine. Tuttavia, occorrerebbe specificare chiaramente le eccezioni, in particolare riguardo all'accesso non esclusivo ai dati concesso al fabbricante o ad autorità pubbliche,

[27] Evidentemente il riferimento del carattere abusivo dei contratti a livello di B2B dovrebbe essere diverso da quello per i contratti B2C, rispecchiando il maggior grado di libertà contrattuale che esiste nelle relazioni di tipo B2B.

ad esempio per la gestione del traffico o per motivi ambientali. Nel caso dei dati personali, la persona interessata conserverà il diritto di revocare il proprio consenso in qualsiasi momento dopo avere autorizzato l'utilizzo. Occorrerebbe rendere anonimi i dati personali, in modo da impedire l'identificazione della persona interessata, prima che l'altra parte possa autorizzarne l'ulteriore utilizzo. In effetti, il regolamento generale sulla protezione dei dati rimane di applicazione per i dati personali (generati da macchine o in altro modo) fino all'anonimizzazione.

- **Accesso dietro compenso**: si potrebbe elaborare un quadro, potenzialmente basato su determinati principi fondamentali quali le condizioni eque, ragionevoli e non discriminatorie (condizioni FRAND), per consentire ai titolari dei dati, quali fabbricanti, prestatori di servizi o di altri soggetti, di fornire accesso ai dati in loro possesso in cambio di remunerazione, previa anonimizzazione dei dati stessi. Occorrerebbe prendere in considerazione i pertinenti legittimi interessi e la necessità di tutelare il segreto commerciale. Si potrebbe anche considerare il ricorso a diversi regimi di accesso per settori e/o modelli commerciali diversi, per tener conto delle peculiarità di ciascun settore. Per esempio, in alcuni casi il libero accesso ai dati (totale o parziale) potrebbe essere la migliore scelta sia per le imprese sia per la società.

La Commissione intende consultare le parti interessate sulle questioni sopra delineate, al fine di raccogliere maggiori informazioni sul funzionamento dei mercati dei dati per settore e di valutare possibili soluzioni. In questo contesto, un ampio dibattito su vasta scala è essenziale per discutere le possibili soluzioni ed evitare effetti indesiderati che soffocherebbero l'innovazione od ostacolerebbero la concorrenza. Si terranno inoltre discussioni con le parti interessate della catena del valore dei dati.

4. RESPONSABILITÀ

Altro tema emergente è l'applicazione delle attuali norme in materia di responsabilità nell'economia dei dati in relazione a prodotti e servizi basati su tecnologie emergenti quali l'internet delle cose (IoT), le fabbriche del futuro e i sistemi autonomi connessi. L'internet delle cose è una rete in rapida espansione di oggetti di uso quotidiano, quali orologi, veicoli e termostati, collegati a internet. I sistemi autonomi connessi, come i veicoli senza conducente, agiscono in modo indipendente dall'intervento umano e sono in grado di comprendere ed interpretare l'ambiente che li circonda. Queste tecnologie emergenti utilizzano sensori per ottenere i vari tipi di dati spesso necessari per il funzionamento del prodotto o del servizio.

Sono tutte innovazioni in grado di migliorare la sicurezza e la qualità della vita, che tuttavia sono inevitabilmente soggette alla possibilità di errori di progettazione, cattivo funzionamento o manipolazione dei dispositivi. I problemi possono insorgere in seguito alla trasmissione di dati erronei da parte di un sensore, ad esempio per vizi del software, problemi di connettività o cattivo funzionamento della macchina. La natura di questi sistemi rende difficile determinare l'esatta provenienza di un problema che abbia provocato danni, sollevando la questione di come garantire la sicurezza per gli utenti riducendo al minimo la possibilità di causare danni, e di chi debba essere ritenuto responsabile dei danni che nonostante tutto dovessero verificarsi.

Le modalità con cui dare certezza sia agli utilizzatori sia ai produttori dei dispositivi in relazione alla loro potenziale responsabilità sono quindi un tema di fondamentale importanza per lo sviluppo di un'economia basata sui dati.

4.1. Norme UE sulla responsabilità

Il diritto civile in generale distingue due tipi di responsabilità legale: la responsabilità contrattuale, in cui la responsabilità per il danno deriva dal rapporto contrattuale tra le parti, e la responsabilità extracontrattuale[28], che è fissata al di fuori del vincolo contrattuale. Un tipo importante di responsabilità extracontrattuale è quella relativa alla responsabilità per danno da prodotti difettosi. A livello dell'UE, la direttiva in materia di responsabilità per danno da prodotti difettosi (85/374/CEE) stabilisce il principio della responsabilità oggettiva, vale a dire la responsabilità senza colpa: nei casi in cui un prodotto difettoso provoca un danno a un consumatore, i fabbricanti possono essere ritenuti responsabili anche senza colpa o negligenza da parte loro. Tuttavia, può risultare difficile o incerto applicare le disposizioni della direttiva[29] nell'ambito dell'internet delle cose e dei sistemi autonomi connessi (ad esempio la robotica), per i seguenti motivi: le caratteristiche di tali sistemi, ad esempio una complessa catena del valore di un prodotto o di un servizio, con interdipendenze tra fornitori, fabbricanti e altri soggetti; l'incertezza sulla natura giuridica dei dispositivi IoT, vale a dire se sono prodotti, servizi o prodotti associati alla vendita di un servizio; il carattere autonomo di tali tecnologie.

La Commissione ha avviato un'ampia valutazione della direttiva sulla responsabilità per i prodotti difettosi, al fine di valutarne globalmente il funzionamento e verificare se le sue disposizioni, elaborate per un ambiente molto diverso, rimangano adatte anche a tecnologie emergenti quali l'internet delle cose e i sistemi autonomi connessi.

4.2. Possibili sviluppi

L'obiettivo della Commissione è rafforzare la certezza del diritto in materia di responsabilità nel contesto delle tecnologie emergenti, creando così condizioni favorevoli per l'innovazione. Oltre al mantenimento dello *status quo*[30], sono stati vagliati diversi approcci, fra cui i seguenti.

- **Approccio della creazione del rischio e approccio della gestione del rischio**: Con questi approcci la responsabilità potrebbe essere assegnata all'operatore del mercato che crea un rischio sostanziale ad altri, oppure all'operatore del mercato che si trova nella posizione migliore per ridurre al minimo o evitare il verificarsi di tale rischio.

---

28 Le norme dell'UE sulla responsabilità riguardano unicamente la responsabilità extracontrattuale.

29 Riferimenti alla responsabilità oggettiva dei produttori in caso di prodotti difettosi si rinvengono in altri atti legislativi in materia di sicurezza dei prodotti, quali ad esempio la direttiva sulle apparecchiature radio (2014/53/UE), i regolamenti sui dispositivi medici, la direttiva "macchine" (2006/42/CE) e la direttiva sulla sicurezza generale dei prodotti (2001/95/CE).

30 La Commissione potrebbe formulare orientamenti sull'applicazione delle norme UE in materia di responsabilità per l'internet delle cose e la robotica.

- **Regimi di assicurazione volontari od obbligatori**: Tali regimi potrebbero andare di pari passo con gli approcci alla responsabilità di cui sopra. Risarcirebbero le parti che hanno subìto il danno (ad esempio, il consumatore). Questo approccio dovrebbe fornire una tutela giuridica agli investimenti delle imprese, rassicurando al contempo le vittime sull'equità del risarcimento o sull'esistenza di un'assicurazione in caso di danni.

Tutti gli approcci dovrebbero tener conto delle azioni della persona che utilizza la tecnologia e identificare in modo più preciso quale debba essere il ruolo degli utilizzatori della medesima tecnologia.

La Commissione consulterà le parti interessate sull'adeguatezza della normativa dell'UE vigente in materia di responsabilità nel contesto dell'internet delle cose e dei sistemi autonomi connessi, nonché su possibili approcci per superare le attuali difficoltà di assegnazione della responsabilità. È inoltre in corso, in parallelo, una consultazione pubblica sulla valutazione globale dell'applicazione della direttiva sulla responsabilità per i prodotti difettosi. La Commissione valuterà i risultati e vaglierà le opzioni per un'azione futura.

5. PORTABILITÀ, INTEROPERABILITÀ E NORMAZIONE

Altre questioni emergenti nell'economia dei dati sono la portabilità dei dati non personali, l'interoperabilità dei servizi per consentire lo scambio di dati e le norme tecniche idonee per l'attuazione di una portabilità effettiva.

5.1. Portabilità dei dati non personali

La portabilità dei dati implica che i consumatori e le imprese possano facilmente trasferire i propri dati da un sistema all'altro. Generalmente è associata a costi di conversione contenuti e, di conseguenza, a barriere d'ingresso minime nell'economia dei dati. Il regolamento generale sulla protezione dei dati conferirà ai singoli il diritto di ricevere i dati personali forniti al prestatore di servizi in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un altro fornitore di servizi[31].

Tuttavia, per i dati non personali attualmente non vi sono obblighi di garantire anche solo un livello minimo di portabilità, anche per servizi online ampiamente utilizzati come la fornitura di hosting su cloud. Ciò è in parte dovuto al fatto che i requisiti di attuazione della portabilità dei dati possono essere tecnicamente complessi e avere costi significativi, dato che diversi fornitori degli stessi servizi possono conservare i dati con modalità diverse.

Un'effettiva portabilità dei dati non personali dovrebbe anche tener conto di più ampie considerazioni di *governance* dei dati in merito alla trasparenza per gli utilizzatori, all'accesso gestito e all'interoperabilità per collegare fra loro diverse piattaforme in modo da stimolare l'innovazione.

[31] Articolo 20.

5.2. Interoperabilità

Spesso le considerazioni sulla portabilità dei dati sono strettamente collegate a questioni di interoperabilità dei dati, che consente a più servizi digitali di scambiare i dati in modo agevole, grazie a specifiche tecniche adatte. La direttiva sull'informazione del settore pubblico e i relativi orientamenti (compreso il quadro europeo di interoperabilità) sottolineano quanto sia importante che metadati standardizzati ingenti seguano vocabolari prestabiliti per facilitare la ricerca e l'interoperabilità. Attualmente ai dati territoriali del settore pubblico[32] si applica la direttiva che istituisce l'infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE) con i relativi regolamenti e orientamenti di interoperabilità per i dati territoriali e i relativi servizi, compresi i dati di osservazione dei sensori.

Nel caso di piattaforme online, l'interoperabilità dei dati non solo agevola il cambiamento di fornitore, ma anche l'uso simultaneo di diverse piattaforme (il cosiddetto "multi-homing"), nonché la generalizzazione dello scambio di dati su più piattaforme, che ha il potenziale di promuovere l'innovazione nell'economia digitale.

5.3. Normazione

Politiche di portabilità efficaci devono appoggiarsi su norme tecniche adeguate per attuare una portabilità effettiva in modo tecnologicamente neutro. La Commissione si è impegnata[33] a sostenere una normazione appropriata per migliorare l'interoperabilità, la portabilità e la sicurezza dei servizi su cloud, mediante una migliore integrazione delle attività delle comunità "open source" per la normazione a livello europeo. Esempi di tale approccio sono la specifica TOSCA per le applicazioni cloud, volta a migliorare la portabilità e la gestione operativa delle applicazioni e dei servizi su cloud[34], e le specifiche e orientamenti tecnici dei regolamenti di attuazione INSPIRE[35].

5.4. Possibili sviluppi

Fra le opzioni possibili in prospettiva per affrontare le suddette questioni si annoverano le seguenti.

- **Elaborare raccomandazioni di condizioni contrattuali per agevolare il cambiamento di fornitore di servizi**: poiché la portabilità dei dati e il cambiamento di fornitore di servizi di dati sono fra loro interdipendenti, si potrebbe prendere in considerazione l'elaborazione di clausole contrattuali standard che impongano al fornitore di servizi di attuare la portabilità dei dati del cliente.

---

32 I dati generati da macchine sono "dati territoriali" perché sensori solitamente trasmettono anche la loro posizione (ubicazione), direttamente o indirettamente, insieme con la misurazione.

33 COM(2016) 176 final: Priorità per la normazione delle TIC per il mercato unico digitale.

34 https://www.oasis-open.org/committees/tosca

35 Atti giuridici INSPIRE: http://inspire.ec.europa.eu/inspire-legislation/26

- **Sviluppare ulteriormente i diritti di portabilità dei dati**: prendendo spunto dal diritto alla portabilità dei dati sancito dal regolamento generale sulla protezione dei dati e dalle norme proposte per i contratti di fornitura di contenuto digitale, si potrebbero introdurre ulteriori diritti alla portabilità dei dati non personali, in particolare per i contesti B2B, tenendo debitamente conto dei risultati del controllo dell'adeguatezza in corso su atti normativi principali dell'UE in materia di commercio e di tutela dei consumatori[36].

- **Esperimenti di normazione a livello settoriale**: per sviluppare un solido approccio a norme di portabilità codificate, si potrebbe avviare un approccio specifico a livello settoriale. Ciò comporterebbe, di norma, una collaborazione tra tutte le parti interessate, compresi gli organismi di normazione, l'industria, la comunità tecnica e le autorità pubbliche.

La Commissione consulterà le parti interessate su tali questioni e valuterà, su tale base, l'eventuale necessità di ulteriori interventi, eventualmente mediante le azioni sopra menzionate, singolarmente o in combinazione fra loro.

6. SPERIMENTAZIONE E PROVE

La sperimentazione è un elemento importante dell'esplorazione delle questioni emergenti nell'economia dei dati. Si valuterà la possibilità di attingere a finanziamenti di Orizzonte 2020 a sostegno di questi tipi di prove ed esperimenti.

Prima di giungere a conclusioni in merito all'idoneità delle possibili soluzioni per l'accesso ai dati e la responsabilità in merito, occorrerebbe organizzare una prova apposita per verificare tali questioni in ambiente reale, in collaborazione con le parti interessate. Occorre trovare una soluzione europea, basata sulla cooperazione e sulla sperimentazione fra gli Stati membri.

A tal fine, si potrebbe prendere in considerazione la mobilità cooperativa, connessa e automatizzata[37], per la sua dimensione transfrontaliera.

Alcuni progetti sono già in corso in diversi Stati membri per sviluppare sistemi cooperativi e livelli di automazione più elevati[38]. I progetti consentono di collegare i veicoli tra loro e con infrastrutture stradali quali semafori e segnaletica. Inoltre, la Commissione intende lavorare con un gruppo di Stati membri interessati a creare un quadro giuridico di verifica per svolgere esperimenti sulla base di norme armonizzate sull'accesso ai dati e sulla responsabilità. Per consentire l'accesso a un volume sufficiente di dati, occorrerebbe basare la sperimentazione sul 5G, operando senza soluzione di continuità con tecnologie già in uso e in base a un principio di complementarietà[39].

---

36 http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

37 Cfr. COM(2016) 766 final, del 30.11.2016.

38 COM(2016) 766 final: Una strategia europea per i sistemi di trasporto intelligenti cooperativi.

39 COM(2016) 588 final: Il 5G per l'Europa: un piano d'azione.

Un'altra interessante sperimentazione proverrà dal settore geospaziale, con l'emergere di un nuovo ecosistema di dati costruito intorno a Copernicus, il programma UE di osservazione della Terra e terzo maggiore fornitore di dati al mondo. La Commissione sta sviluppando soluzioni innovative per favorire lo sviluppo di applicazioni basate su Copernicus e su altri dati territoriali, in particolare affrontando le questioni dell'accesso ai dati, dell'interoperabilità e della prevedibilità.

7. CONCLUSIONE

Per costruire l'economia dei dati, l'UE necessita di un assetto programmatico che consenta di utilizzare i dati in tutta la catena di valore per fini scientifici, sociali e industriali. A tal fine, la Commissione sta avviando un ampio dialogo con le parti interessate in merito alle questioni esaminate nella presente comunicazione. Il primo passo di questo dialogo sarà una consultazione pubblica. Le questioni relative all'accesso ai dati e alla responsabilità saranno inoltre oggetto di sperimentazione in ambiente reale nel settore della mobilità cooperativa, connessa e automatizzata.

Per quanto riguarda il libero flusso dei dati, la Commissione continuerà a impegnarsi su tale questione in linea con l'approccio sopra descritto, per applicare pienamente il principio della libera circolazione dei dati all'interno dell'UE, anche, ove necessario e opportuno, tramite azioni prioritarie di controllo dell'osservanza. La Commissione continuerà inoltre a monitorare la situazione e raccogliere elementi e, se necessario, prenderà in considerazione ulteriori iniziative sul libero flusso dei dati.

Sulla base dei risultati del dialogo con le parti interessate, la Commissione valuterà anche l'opportunità di ulteriori interventi sui problemi emergenti e proporrà soluzioni pertinenti. In tale contesto, si potrebbe avere un contributo anche dalla sperimentazione in condizioni reali.