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

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) L'economia si sta velocemente digitalizzando. Le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni. I dati elettronici sono al centro di tali sistemi e, quando sono analizzati o utilizzati in associazione a servizi e prodotti, possono generare un ingente valore. Allo stesso tempo, il rapido sviluppo dell'economia dei dati e di tecnologie emergenti come l'intelligenza artificiale, i prodotti e i servizi relativi all'Internet degli oggetti, i sistemi autonomi e la tecnologia 5G sollevano nuove questioni giuridiche relative all'accesso ai dati e al loro riutilizzo, alla responsabilità, all'etica e alla solidarietà. Si dovrebbe considerare l'opportunità di lavorare in materia di responsabilità, segnatamente attraverso l'impiego di codici di autoregolamentazione e altre migliori prassi, tenendo conto delle raccomandazioni, delle decisioni e delle azioni adottate senza interazione umana lungo l'intera catena del valore del trattamento dei dati. Tali lavori potrebbero anche contemplare meccanismi appropriati per determinare la responsabilità, per trasferire la responsabilità tra servizi che cooperano, per l'assicurazione e per l'audit.

(2) Le catene del valore dei dati sono il risultato di diverse attività relative ai dati: la creazione e la raccolta; l'aggregazione e l'organizzazione; il trattamento; l'analisi, la commercializzazione e la distribuzione; l'utilizzo e il riutilizzo. Il funzionamento efficace ed efficiente del trattamento di dati costituisce un elemento fondamentale di qualsiasi catena del valore dei dati. Eppure, tale trattamento di dati efficace ed efficiente e l'evoluzione dell'economia dei dati nell'Unione sono compromessi principalmente da due tipi di ostacoli relativi alla mobilità dei dati e al mercato interno: gli obblighi in materia di localizzazione dei dati posti in essere dalle autorità degli Stati membri e pratiche di «vendor lock-in» nel settore privato.

(3) La libertà di stabilimento e la libertà di fornire servizi in virtù del trattato sul funzionamento dell'Unione europea (TFUE) si applicano ai servizi di trattamento di dati. Tuttavia, la prestazione di tali servizi è ostacolata – ove non impedita – da alcune disposizioni nazionali, regionali o locali che impongono obblighi di localizzazione dei dati in un determinato territorio.

(4) Tali ostacoli alla libera circolazione dei servizi di trattamento di dati e al diritto di stabilimento dei fornitori di servizi di trattamento di dati discendono da disposizioni contenute nelle legislazioni degli Stati membri che impongono obblighi di localizzazione dei dati a fini di trattamento di dati in una determinata area geografica o territorio. Altre norme o pratiche amministrative hanno un effetto equivalente quando introducono requisiti specifici che rendono più difficile trattare dati al di fuori di un determinato territorio o area geografica all'interno dell'Unione, ad esempio l'obbligo di utilizzare dispositivi tecnologici che siano certificati o omologati in un determinato Stato membro. L'incertezza giuridica circa la portata degli obblighi – giustificati o ingiustificati – di localizzazione dei dati limita ulteriormente le scelte disponibili agli operatori del mercato e del settore pubblico per quanto riguarda la localizzazione dei dati trattati. 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.

([1]) GU C 227 del 28.6.2018, pag. 78.
([2]) Posizione del Parlamento europeo del 4 ottobre 2018 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 6 novembre 2018.

(5) Allo stesso tempo, la mobilità dei dati all'interno dell'Unione è anche ostacolata da restrizioni relative al settore privato, quali aspetti giuridici, contrattuali e tecnici che ostacolano o impediscono agli utenti di servizi di trattamento di dati di trasferire i propri dati da un fornitore di servizi a un altro o di ritrasferirli verso i propri sistemi informatici, non da ultimo al termine del loro contratto con il fornitore di servizi.

(6) La combinazione di tali ostacoli ha determinato una mancanza di concorrenza tra i fornitori di servizi cloud nell'Unione, diversi problemi di «vendor lock-in» e gravi carenze in termini di mobilità dei dati. Analogamente, le politiche di localizzazione dei dati hanno compromesso la capacità delle aziende di ricerca e sviluppo di agevolare la collaborazione tra imprese, università e altre organizzazioni di ricerca allo scopo di sostenere l'innovazione.

(7) Un unico insieme di regole per tutti i partecipanti al mercato costituisce un elemento essenziale per il corretto funzionamento del mercato interno, affinché siano garantite la certezza del diritto e la parità di condizioni all'interno dell'Unione. Al fine di rimuovere gli ostacoli agli scambi ed evitare distorsioni della concorrenza derivanti da divergenti normative nazionali, nonché per prevenire il probabile insorgere di ulteriori ostacoli e distorsioni significative, è necessario adottare norme uniformi applicabili in tutti gli Stati membri.

(8) Il quadro giuridico relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche, e segnatamente il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([1]), nonché le direttive (UE) 2016/680 ([2]) e 2002/58/CE ([3]) del Parlamento europeo e del Consiglio, non sono pregiudicati dal presente regolamento.

(9) L'espansione dell'Internet degli oggetti, l'intelligenza artificiale e l'apprendimento automatico rappresentano fonti importanti di dati non personali, ad esempio a seguito del loro utilizzo in processi automatizzati di produzione industriale. Fra gli esempi specifici di dati non personali figurano gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati, i dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua, o i dati sulle esigenze di manutenzione delle macchine industriali. Se i progressi tecnologici consentono di trasformare dati anonimizzati in dati personali, tali dati sono trattati come dati personali e si applica di conseguenza il regolamento (UE) 2016/679.

(10) A norma del regolamento (UE) 2016/679, gli Stati membri non possono limitare o vietare la libera circolazione dei dati personali all'interno dell'Unione per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento di dati personali. Il presente regolamento sancisce il medesimo principio di libera circolazione all'interno dell'Unione per i dati non personali, tranne nei casi in cui una limitazione o un divieto sono giustificati per motivi di sicurezza pubblica. 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. Inoltre, il presente regolamento non impone l'obbligo di archiviare separatamente i diversi tipi di dati.

(11) Per istituire un quadro applicabile alla libera circolazione dei dati non personali nell'Unione e creare il fondamento per lo sviluppo dell'economia dei dati e il rafforzamento della competitività dell'industria dell'Unione, è necessario stabilire regole giuridiche chiare, complete e prevedibili per il trattamento di dati diversi dai dati personali nel mercato interno. Un approccio basato sui principi che preveda la cooperazione tra gli Stati membri e l'autoregolamentazione dovrebbe garantire un quadro normativo sufficientemente flessibile da poter tener conto dell'evoluzione delle esigenze degli utenti, dei fornitori di servizi e delle autorità nazionali nell'Unione. Onde evitare il rischio di sovrapposizioni con i meccanismi esistenti e, di conseguenza, oneri maggiori sia per gli Stati membri che per le imprese, è opportuno non introdurre norme tecniche dettagliate.

(12) Il presente regolamento non dovrebbe pregiudicare il trattamento di dati, nella misura in cui questo è effettuato nell'ambito di un'attività che non è disciplinata dal diritto dell'Unione. In particolare, è opportuno rammentare che a norma dell'articolo 4 del trattato sull'Unione europea (TUE), la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro.

([1]) 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 (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([2]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

([3]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento di dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

(13) La libera circolazione dei dati nell'Unione svolgerà un ruolo importante nel raggiungere una crescita e un'innovazione basate sui dati. Come le imprese e i consumatori, anche le autorità pubbliche e gli organismi di diritto pubblico degli Stati membri traggono beneficio da una maggiore libertà di scelta per quanto riguarda i fornitori di servizi basati sui dati, da prezzi più competitivi e da una maggiore efficienza nella prestazione di servizi ai cittadini. Considerata la grande quantità di dati che le autorità e gli organismi di diritto pubblico gestiscono, è estremamente importante che essi diano l'esempio avvalendosi di servizi di trattamento dei dati e si astengano dall'applicare restrizioni alla localizzazione dei dati quando utilizzano i servizi di trattamento dei dati. Pertanto, le autorità e gli organismi di diritto pubblico dovrebbero essere contemplati dal presente regolamento. A tale riguardo, il principio della libera circolazione dei dati non personali di cui al presente regolamento dovrebbe applicarsi inoltre alle prassi amministrative generali e coerenti e ad altri requisiti di localizzazione dei dati nel settore degli appalti pubblici, fatta salva la direttiva 2014/24/UE del Parlamento europeo e del Consiglio ([1]).

(14) Come la direttiva 2014/24/UE, il presente regolamento fa salve le disposizioni legislative, regolamentari e amministrative relative all'organizzazione interna degli Stati membri che assegnano tra autorità pubbliche e organismi di diritto pubblico poteri e responsabilità in materia di trattamento dei dati senza remunerazione contrattuale di soggetti privati nonché le disposizioni legislative, regolamentari e amministrative degli Stati membri che regolano l'esercizio di tali poteri e responsabilità. 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.

(15) Il presente regolamento dovrebbe applicarsi alle persone fisiche o giuridiche che forniscono servizi di trattamento di dati a utenti residenti o stabiliti nell'Unione, comprese quelle che forniscono servizi di trattamento di dati nell'Unione senza esservi stabilite. Il presente regolamento non dovrebbe pertanto applicarsi ai servizi di trattamento di dati svolti al di fuori dell'Unione e ai requisiti di localizzazione relativi a tali dati.

(16) Il presente regolamento non stabilisce norme relative alla determinazione della legge applicabile in materia commerciale e lascia pertanto impregiudicato il regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio ([2]). In particolare, nella misura in cui la legge applicabile a un contratto non è stata scelta a norma di tale regolamento, il contratto di prestazione di servizi è disciplinato, in linea di principio, dalla legge del paese in cui il prestatore di servizi ha la residenza abituale.

(17) Il presente regolamento dovrebbe intendere i trattamenti di dati nell'accezione più ampia possibile, indipendentemente dal tipo di sistema della tecnologia dell'informazione utilizzato e sia che tali operazioni siano effettuate nei locali dell'utente o siano esternalizzate ad un fornitore di servizi. Esso dovrebbe contemplare il trattamento di dati a diversi livelli di intensità, dall'archiviazione (Infrastructure-as-a-Service - IaaS) al trattamento di dati su piattaforme (Platform-as-a-Service - PaaS) o in applicazioni (Software-as-a-Service - SaaS).

(18) Gli obblighi di localizzazione dei dati costituiscono un chiaro ostacolo alla libera prestazione di servizi di trattamento di dati in tutta l'Unione e al mercato interno. In quanto tali, dovrebbero essere vietati tranne quando siano giustificati da motivi di pubblica sicurezza, ai sensi del diritto dell'Unione, in particolare ai sensi dell'articolo 52 TFUE, e soddisfino il principio di proporzionalità sancito dall'articolo 5 TUE. Al fine di dare concreta attuazione al principio della libera circolazione transfrontaliera dei dati non personali, assicurare la rapida rimozione degli obblighi di localizzazione dei dati esistenti e consentire, per motivi operativi, il trattamento di dati in più località distribuite nel territorio dell'Unione, e atteso che il presente regolamento prevede misure per garantire la disponibilità dei dati ai fini del controllo di regolamentazione, è opportuno che gli Stati membri possano invocare unicamente la sicurezza pubblica come giustificazione per gli obblighi di localizzazione dei dati.

(19) La nozione di «pubblica sicurezza» ai sensi dell'articolo 52 TFUE, nell'interpretazione datane dalla Corte di giustizia, riguarda la sicurezza sia interna che esterna di uno Stato membro, come pure le questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati. Presuppone l'esistenza di una minaccia reale e sufficientemente grave a uno degli interessi fondamentali della società, quale 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. Conformemente al principio di proporzionalità, gli obblighi di localizzazione dei dati giustificati da motivi imperativi di pubblica sicurezza dovrebbero essere adatti al raggiungimento dell'obiettivo perseguito e limitarsi a quanto è necessario per conseguire tale obiettivo.

([1]) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

([2]) Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I) (GU L 177 del 4.7.2008, pag. 6).

(20) Per garantire l'efficace applicazione del principio della libera circolazione transfrontaliera di dati non personali ed evitare l'insorgere di nuovi ostacoli al corretto funzionamento del mercato interno, è opportuno che gli Stati membri comunichino immediatamente alla Commissione qualsiasi progetto di atto che introduca un nuovo obbligo di localizzazione dei dati o ne modifichi uno esistente. Tali progetti di atto dovrebbero essere presentati e valutati conformemente alla direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([1]).

(21) Inoltre, onde eliminare le potenziali barriere esistenti è opportuno che gli Stati membri procedano, nel corso di un periodo transitorio di 24 mesi a decorrere dalla data di applicazione del presente regolamento, al riesame delle vigenti disposizioni legislative, regolamentari e amministrative di carattere generale che stabiliscono gli obblighi di localizzazione dei dati e che comunichino alla Commissione tutti gli obblighi di localizzazione dei dati che ritengono conformi al presente regolamento, corredandoli della giustificazione. Ciò dovrebbe consentire alla Commissione di esaminare la conformità di tutti i rimanenti obblighi di localizzazione dei dati. È opportuno attribuire alla Commissione la facoltà, ove opportuno, di presentare osservazioni allo Stato membro in questione. Tali osservazioni potrebbero contemplare la raccomandazione di modificare o abrogare l'obbligo di localizzazione dei dati.

(22) L'obbligo di comunicare alla Commissione gli obblighi vigenti di localizzazione dei dati e i relativi progetti di atti, stabilito dal presente regolamento, dovrebbe applicarsi agli obblighi regolamentari di localizzazione dei dati e ai progetti di atti di natura generale, ma non alle decisioni rivolte a una persona fisica o giuridica specifica.

(23) Al fine di garantire la trasparenza degli obblighi di localizzazione dei dati negli Stati membri stabiliti in disposizioni legislative, regolamentari o amministrative di natura generale per le persone fisiche e giuridiche, quali fornitori di servizi e utenti di servizi di trattamento di dati, gli Stati membri dovrebbero pubblicare le informazioni relative a tali obblighi in un portale unico nazionale on line d'informazione, che sarà aggiornato periodicamente. In alternativa gli Stati membri dovrebbero fornire tali informazioni aggiornate in merito a tali obblighi presso un portale informazioni centralizzato istituito da un altro atto dell'Unione. Per informare adeguatamente le persone fisiche e giuridiche sugli obblighi di localizzazione dei dati in tutta l'Unione, è opportuno che gli Stati membri comunichino alla Commissione l'indirizzo di detti portali unici d'informazione. La Commissione dovrebbe pubblicare tali informazioni sul suo sito web insieme a un elenco consolidato, aggiornato periodicamente, di tutti gli obblighi di localizzazione dei dati in vigore negli Stati membri, comprendente informazioni sintetiche su detti obblighi.

(24) Gli obblighi di localizzazione dei dati derivano spesso dalla mancanza di fiducia nelle operazioni transfrontaliere di trattamento di dati, dovuta alla presunta indisponibilità dei dati alle autorità competenti degli Stati membri per l'esercizio delle loro funzioni, quali l'ispezione e l'audit nell'ambito di un controllo regolamentare o di vigilanza. Tale mancanza di fiducia non può essere superata soltanto con la nullità delle clausole contrattuali che vietano l'accesso legittimo ai dati da parte delle autorità competenti per l'esercizio delle loro funzioni ufficiali. Pertanto, il presente regolamento dovrebbe precisare chiaramente che esso non pregiudica la facoltà delle autorità competenti di chiedere od ottenere l'accesso ai dati conformemente al diritto dell'Unione o nazionale, e che tale accesso non può essere rifiutato alle autorità competenti per il fatto che i dati sono trattati in un altro Stato membro. Le autorità competenti potrebbero imporre requisiti funzionali a sostegno dell'accesso ai dati, come ad esempio l'obbligo di conservare le descrizioni del sistema nello Stato membro interessato.

(25) Le persone fisiche o giuridiche che sono tenute a fornire dati alle autorità competenti possono conformarsi a tali obblighi fornendo e garantendo alle autorità competenti l'accesso elettronico effettivo e tempestivo ai dati, indipendentemente dallo Stato membro nel cui territorio i dati sono trattati. Tale accesso può essere garantito da clausole e condizioni contrattuali stipulate tra la persona fisica o giuridica soggetta all'obbligo di garantire l'accesso e il fornitore di servizi.

(26) Quando una persona fisica o giuridica è soggetta a un obbligo di fornire i dati e non vi ottempera, l'autorità competente dovrebbe poter chiedere assistenza alle autorità competenti di altri Stati membri. In tali casi, è opportuno che le autorità competenti utilizzino gli specifici strumenti di cooperazione previsti dal diritto dell'Unione o a norma di accordi internazionali, ad esempio, a seconda della materia trattata, rispettivamente nel

([1]) 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 (GU L 241 del 17.9.2015, pag. 1).

settore della cooperazione di polizia, penale o civile o amministrativa: la decisione quadro 2006/960/GAI del Consiglio ([1]), la direttiva 2014/41/UE del Parlamento europeo e del Consiglio ([2]), la Convenzione sulla criminalità informatica del Consiglio d'Europa ([3]), il regolamento (CE) n. 1206/2001 del Consiglio ([4]), la direttiva 2006/112/CE del Consiglio ([5]) e il regolamento (UE) n. 904/2010 del Consiglio ([6]). In mancanza di tali meccanismi specifici di cooperazione, le autorità competenti dovrebbero cooperare tra loro in modo da fornire l'accesso ai dati richiesti per il tramite dei punti di contatto unici designati.

(27) Se una richiesta di assistenza comporta che l'autorità richiesta ottenga l'accesso a tutti i locali di una persona fisica o giuridica, compresi tutti gli strumenti e dispositivi di trattamento di dati, tale accesso deve essere conforme al diritto dell'Unione o alle norme procedurali nazionali, compreso l'eventuale obbligo di ottenere una previa autorizzazione giudiziaria.

(28) Il presente regolamento non dovrebbe consentire agli utilizzatori di tentare di eludere l'applicazione del diritto nazionale. È pertanto opportuno adottare disposizioni affinché gli Stati membri impongano sanzioni effettive, proporzionate e dissuasive agli utenti che impediscono alle autorità competenti di accedere ai propri dati, necessari alle autorità competenti per l'esercizio delle loro funzioni ufficiali a norma del diritto dell'Unione e nazionale. In casi urgenti, qualora un utente abusi del proprio diritto, gli Stati membri dovrebbero poter imporre misure provvisorie rigorosamente proporzionate. Eventuali misure provvisorie che richiedano la rilocalizzazione dei dati per un periodo superiore a 180 giorni dopo la rilocalizzazione si discosterebbero dal principio della libera circolazione dei dati per un periodo significativo e dovrebbero pertanto essere comunicate alla Commissione ai fini dell'esame della loro compatibilità con il diritto dell'Unione.

(29) La portabilità dei dati senza impedimenti è uno degli elementi fondamentali che agevolano la scelta degli utenti e stimolano la concorrenza effettiva nei mercati dei servizi di trattamento di dati. Inoltre le difficoltà reali o percepite relative alla portabilità transfrontaliera dei dati compromettono la fiducia degli utenti professionali nelle offerte transfrontaliere, e di conseguenza, la loro fiducia nel mercato interno. Mentre i consumatori singoli traggono vantaggi dal vigente diritto dell'Unione, essa non facilita gli utenti che intendono cambiare fornitore di servizi nell'ambito della loro attività imprenditoriale o professionale. Anche l'adozione di requisiti tecnici coerenti in tutta l'Unione, per quanto riguarda l'armonizzazione tecnica, il riconoscimento reciproco o l'armonizzazione volontaria, contribuisce allo sviluppo di un mercato interno competitivo per i servizi di trattamento dati.

(30) Perché possano trarre pienamente vantaggio dall'ambiente concorrenziale, è opportuno che gli utenti professionali siano in grado di compiere scelte informate e di confrontare facilmente i singoli elementi dei servizi di trattamento di dati offerti nel mercato interno, anche sotto il profilo delle clausole e condizioni contrattuali di portabilità dei dati al termine del contratto. Per 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, le informazioni dettagliate e i requisiti operativi per la portabilità dei dati dovrebbero essere definiti dagli operatori del mercato mediante autoregolamentazione, incoraggiati, agevolati e controllati dalla Commissione, in forma di codici di condotta dell'Unione che potrebbero contemplare clausole e condizioni contrattuali tipo.

(31) Per essere efficaci e facilitare il cambio tra fornitori di servizi e la portabilità dei dati, tali codici di condotta dovrebbero essere esaustivi e riguardare almeno gli aspetti fondamentali che sono importanti durante il processo di portabilità dei dati, quali le procedure per e il luogo in cui è effettuato il backup dei dati, i formati e i supporti dei dati disponibili, la configurazione informatica e la larghezza minima di banda della rete richieste, il tempo necessario per avviare la procedura di trasferimento dei dati e il periodo in cui i dati saranno disponibili per il trasferimento, nonché le garanzie di accesso ai dati in caso di fallimento del fornitore di servizi. I codici di condotta dovrebbero altresì chiarire che le pratiche di «vendor lock-in» non sono pratiche commerciali accettabili, prevedere tecnologie che incrementino la fiducia ed essere periodicamente aggiornati per restare al passo con gli sviluppi tecnologici. La Commissione dovrebbe garantire che tutte le parti interessate, incluse le associazioni di piccole e medie imprese (PMI) e le start-up, gli utenti e i fornitori di servizi cloud siano consultate durante tutte le fasi del processo. La Commissione dovrebbe valutare l'elaborazione e l'efficacia dell'attuazione di tali codici di condotta.

([1]) Decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006, relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge (GU L 386 del 29.12.2006, pag. 89).

([2]) Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale (GU L 130 dell'1.5.2014, pag. 1).

([3]) Convenzione sulla criminalità informatica del Consiglio d'Europa, STCE n. 185.

([4]) Regolamento (CE) n. 1206/2001 del Consiglio, del 28 maggio 2001, relativo alla cooperazione fra le autorità giudiziarie degli Stati membri nel settore dell'assunzione delle prove in materia civile o commerciale (GU L 174 del 27.6.2001, pag. 1).

([5]) Direttiva 2006/112/CE del Consiglio, del 28 novembre 2006, relativa al sistema comune d'imposta sul valore aggiunto (GU L 347 dell'11.12.2006, pag. 1).

([6]) Regolamento (UE) n. 904/2010 del Consiglio, del 7 ottobre 2010, relativo alla cooperazione amministrativa e alla lotta contro la frode in materia d'imposta sul valore aggiunto (GU L 268 del 12.10.2010, pag. 1).

(32) Quando un'autorità competente di uno Stato membro chiede l'assistenza di un altro Stato membro per avere accesso ai dati sulla base del presente regolamento, dovrebbe presentare al punto di contatto unico di quest'ultimo, per il tramite del punto di contatto unico designato, una richiesta debitamente giustificata, che dovrebbe contenere una illustrazione scritta dei motivi e delle basi giuridiche per accedere ai dati. Il punto di contatto unico designato dallo Stato membro a cui è richiesta l'assistenza dovrebbe facilitare la trasmissione della richiesta all'autorità competente nello Stato membro richiesto. Onde garantire una cooperazione efficace, l'autorità richiesta dovrebbe fornire tempestivamente l'assistenza richiesta o fornire informazioni sulle difficoltà incontrate nel soddisfare tale richiesta di assistenza o sui motivi del rifiuto di tale richiesta.

(33) Rafforzare la fiducia nella sicurezza del trattamento transfrontaliero dei dati dovrebbe ridurre la tendenza degli operatori del mercato e del settore pubblico a servirsi della localizzazione dei dati come sostituto della sicurezza dei dati. Dovrebbe inoltre migliorare la certezza del diritto per le imprese circa il rispetto degli obblighi di sicurezza applicabili in caso di esternalizzazione delle loro attività di trattamento di dati a fornitori di servizi, inclusi i fornitori in altri Stati membri.

(34) I requisiti di sicurezza connessi al trattamento di dati che sono applicati in modo giustificato e proporzionato sulla base del diritto dell'Unione o del diritto nazionale nel rispetto del diritto dell'Unione nello Stato membro di residenza o di stabilimento delle persone fisiche o giuridiche i cui dati sono interessati dovrebbero continuare ad applicarsi al trattamento di dati in un altro Stato membro. Tali persone fisiche o giuridiche dovrebbero poter soddisfare tali requisiti direttamente o attraverso clausole contrattuali stabilite nei contratti con i fornitori di servizi.

(35) I requisiti di sicurezza stabiliti a livello nazionale dovrebbero essere necessari e proporzionati ai rischi che corre la sicurezza del trattamento di dati nell'ambito di applicazione del diritto nazionale in cui tali requisiti sono stabiliti.

(36) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([1]) prevede misure giuridiche per rafforzare il livello generale della sicurezza informatica dell'Unione. I servizi di trattamento di dati costituiscono uno dei servizi digitali contemplati da tale direttiva. In base a tale direttiva, gli Stati membri sono tenuti a provvedere affinché i fornitori di servizi digitali identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano. Tali misure sono intese a garantire un livello di sicurezza adeguato al rischio esistente e dovrebbero tenere conto della sicurezza dei sistemi e degli impianti, del trattamento degli incidenti, della gestione della continuità operativa, del monitoraggio, degli audit e test e della conformità con le norme internazionali. Questi elementi devono essere ulteriormente specificati dalla Commissione mediante atti di esecuzione in base a tale direttiva.

(37) È opportuno che la Commissione presenti una relazione sull'attuazione delle disposizioni del presente regolamento, in particolare per valutare la necessità di modificarle in funzione dell'evoluzione delle tecnologie o del mercato. Tale relazione dovrebbe in particolare valutare il presente regolamento, in particolare per quanto riguarda la sua applicazione agli insiemi di dati composti sia da dati personali che da dati non personali, nonché l'attuazione dell'eccezione relativa ai motivi di pubblica sicurezza. Prima che il presente regolamento inizi ad applicarsi, la Commissione dovrebbe inoltre pubblicare orientamenti informativi su come gestire gli insiemi di dati composti sia da dati personali che da dati non personali, affinché le società, tra cui le PMI, comprendano meglio l'interazione tra il presente regolamento e il regolamento (UE) 2016/679 e garantiscano il rispetto di entrambi.

(38) Il presente regolamento rispetta i diritti fondamentali e osserva i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea e dovrebbe essere interpretato e applicato conformemente a tali diritti e principi, principalmente il diritto alla protezione dei dati di carattere personale, la libertà d'espressione e di informazione e la libertà d'impresa.

(39) Poiché l'obiettivo del presente regolamento, segnatamente garantire la libera circolazione dei dati diversi dai dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della sua portata e dei suoi effetti, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 TUE. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

([1]) 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).

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto

Il presente regolamento mira a garantire la libera circolazione dei dati diversi dai dati personali all'interno dell'Unione stabilendo disposizioni relative agli obblighi di localizzazione dei dati, alla messa a disposizione dei dati alle autorità competenti e alla portabilità dei dati per gli utenti professionali.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica alle attività di trattamento di dati elettronici diversi dai dati personali nell'Unione che:

a) sono fornite come servizio ad utenti residenti o stabiliti nell'Unione, indipendentemente dal fatto che il fornitore di servizi sia o non sia stabilito nell'Unione, o

b) sono effettuate da una persona fisica o giuridica residente o stabilito nell'Unione per le proprie esigenze.

2. Nel caso di un insieme di dati composto sia da dati personali che da dati non personali, il presente regolamento si applica alla parte dell'insieme contenente i dati non personali. Qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati, il presente regolamento lascia impregiudicata l'applicazione del regolamento (UE) 2016/679.

3. Il presente regolamento non si applica alle attività che non rientrano nell'ambito di applicazione del diritto dell'Unione.

Il presente regolamento fa salve le disposizioni legislative, regolamentari e amministrative relative all'organizzazione interna degli Stati membri che attribuiscono tra autorità pubbliche e organismi di diritto pubblico quali definiti all'articolo 2, paragrafo 1, punto 4 della direttiva 2014/24/UE poteri e responsabilità in materia di trattamento dei dati, senza remunerazione contrattuale di soggetti privati, nonché le disposizioni legislative, regolamentari e amministrative degli Stati membri che prevedono l'esercizio di tali poteri e responsabilità.

Articolo 3

Definizioni

Ai fini del presente regolamento si intende per:

1) «dati»: i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679;

2) «trattamento»: qualsiasi operazione o insieme di operazioni compiute su dati o insiemi di dati in formato elettronico, con o senza l'ausilio di strumenti automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, il reperimento, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, l'allineamento o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «progetto di atto»: un testo redatto con l'obiettivo di farlo adottare come legge, regolamento o disposizione amministrativa di carattere generale; il testo si trova ancora in fase di preparazione e può ancora essere oggetto di modifiche sostanziali;

4) «fornitore di servizi»: una persona fisica o giuridica che fornisce servizi di trattamento di dati;

5) «obbligo di localizzazione dei dati»: qualsiasi obbligo, divieto, condizione, limite o altro requisito, previsto dalle disposizioni legislative, regolamentari o amministrative di uno Stato membro o risultante dalle prassi amministrative generali e coerenti in uno Stato membro e negli organismi di diritto pubblico, anche nell'ambito degli appalti pubblici, fatta salva la direttiva 2014/24/UE, che impone di effettuare il trattamento di dati nel territorio di un determinato Stato membro o che ostacola il trattamento di dati in un altro Stato membro;

6) «autorità competente»: un'autorità di uno Stato membro o qualsiasi altro ente autorizzato, in virtù del diritto nazionale, a esercitare una funzione pubblica o a esercitare i pubblici poteri, che ha la facoltà di ottenere accesso ai dati trattati da una persona fisica o giuridica ai fini dell'esercizio delle sue funzioni ufficiali, come previsto dal diritto dell'Unione o nazionale;

7) «utente»: una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati;

8) «utente professionale»: 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.

Articolo 4

Libera circolazione dei dati all'interno dell'Unione

1. 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.

2. Gli Stati membri comunicano immediatamente alla Commissione qualsiasi progetto di atto che introduca un nuovo obbligo di localizzazione di dati o apporti modifiche a un vigente obbligo di localizzazione dei dati, in conformità con le procedure stabilite agli articoli 5, 6 e 7 della direttiva (UE) 2015/1535.

3. Entro il 30 maggio 2021, gli Stati membri provvedono a abrogare qualsiasi obbligo di localizzazione dei dati vigente stabilito da una legge, da un regolamento o da una disposizione amministrativa di carattere generale che non sia conforme al paragrafo 1 del presente articolo.

Entro il 30 maggio 2021, se uno Stato membro ritiene che una vigente misura contenente un obbligo di localizzazione dei dati sia conforme al paragrafo 1 del presente articolo e possa pertanto rimanere in vigore, esso comunica tale misura alla Commissione, giustificandone il mantenimento in vigore. Fatto salvo l'articolo 258 TFUE, la Commissione, entro un termine di sei mesi dalla data di ricevimento della comunicazione, esamina la conformità della misura con il paragrafo 1 del presente articolo e, se del caso, presenta osservazioni allo Stato membro interessato, ove necessario, con la raccomandazione di modificare o abrogare la misura.

4. Gli Stati membri rendono pubbliche informazioni dettagliate sugli obblighi di localizzazione dei dati stabiliti da una legge, da un regolamento o da una disposizione amministrativa di carattere generale e applicabili nel loro territorio mediante un portale unico nazionale on line che tengono aggiornato oppure forniscono informazioni aggiornate circa tali obblighi di localizzazione dei dati a un punto informativo centrale istituito da un altro atto dell'Unione.

5. Gli Stati membri comunicano alla Commissione l'indirizzo del loro portale unico di informazioni di cui al paragrafo 4. La Commissione pubblica tali indirizzi sul proprio sito web, insieme a un elenco consolidato e periodicamente aggiornato di tutti gli obblighi di localizzazione dei dati di cui al paragrafo 4, comprese informazioni sintetiche su tali obblighi.

Articolo 5

Messa a disposizione di dati alle autorità competenti

1. Il presente regolamento non pregiudica la facoltà delle autorità competenti di chiedere od ottenere l'accesso a dati ai fini dell'esercizio delle loro funzioni ufficiali conformemente al diritto dell'Unione o nazionale. L'accesso ai dati da parte delle autorità competenti non può essere rifiutato per il fatto che i dati sono trattati in un altro Stato membro.

2. Qualora, dopo avere richiesto l'accesso ai dati di un utente, un'autorità competente non ottenga tale accesso e qualora non esista un meccanismo specifico di cooperazione in base al diritto dell'Unione o ad accordi internazionali per lo scambio di dati tra autorità competenti di diversi Stati membri, detta autorità competente può chiedere l'assistenza di un'autorità competente in un altro Stato membro secondo la procedura di cui all'articolo 7.

3. Se una richiesta di assistenza implica che l'autorità richiesta ottenga l'accesso a tutti i locali di una persona fisica o giuridica, compresi tutti gli strumenti e dispositivi di trattamento di dati, tale accesso deve essere conforme al diritto dell'Unione o alle norme procedurali a livello nazionale.

4. Gli Stati membri possono imporre sanzioni effettive, proporzionate e dissuasive per il mancato rispetto di un obbligo di fornire dati conformemente al diritto nazionale e dell'Unione.

Qualora un utente abusi del proprio diritto, uno Stato membro può imporre a tale utente misure provvisorie rigorosamente proporzionate, ove giustificato dall'urgenza di accedere ai dati e tenendo conto degli interessi delle parti interessate. Se una misura provvisoria prevede la rilocalizzazione dei dati per un periodo superiore a 180 giorni dalla rilocalizzazione, la Commissione ne è informata entro tale periodo di 180 giorni. La Commissione esamina la misura e la sua compatibilità con il diritto dell'Unione nel più breve tempo possibile e, se del caso, adotta le misure necessarie. La Commissione scambia informazioni circa le esperienze in tal senso con i punti di contatto unici degli Stati membri di cui all'articolo 7.

Articolo 6

Portabilità dei dati

1. La Commissione incoraggia e facilita l'elaborazione di codici di condotta di autoregolamentazione a livello dell'Unione («codici di condotta»), al fine di contribuire a un'economia dei dati competitiva basata sui principi della trasparenza e dell'interoperabilità e nell'ambito della quale si tenga debitamente conto degli standard aperti, contemplando, tra l'altro, gli aspetti seguenti:

a) le migliori prassi per agevolare il cambio di fornitore di servizi e la portabilità dei dati in un formato strutturato, di uso comune e leggibile elettronicamente, anche in formati standard aperti ove necessario o richiesto dal fornitore di servizi che riceve i dati;

b) gli obblighi d'informazione minimi per garantire che gli utenti professionali ricevano informazioni sufficientemente dettagliate, chiare e trasparenti prima della conclusione di un contratto di trattamento di dati, per quanto riguarda le procedure e i requisiti tecnici, i tempi e gli oneri applicati nel caso in cui un utente professionale intenda cambiare fornitore di servizi o ritrasferire i dati nei propri sistemi informatici;

c) gli approcci in materia di sistemi di certificazione che agevolano il confronto di prodotti e servizi di trattamento dei dati per gli utenti professionali, tenendo conto delle norme consolidate a livello nazionale o internazionale che agevolano la comparabilità di tali prodotti e servizi. Tali approcci possono includere, tra l'altro, la gestione della qualità, la gestione della sicurezza delle informazioni, la gestione della continuità operativa e la gestione ambientale.

d) tabelle di marcia in materia di comunicazione, con un approccio multidisciplinare volto a sensibilizzare i portatori di interessi a proposito dei codici di condotta.

2. La Commissione provvede affinché i codici di condotta siano elaborati in stretta cooperazione con tutti i portatori di interesse, tra cui le associazioni di PMI e start-up, gli utenti e i fornitori di servizi cloud.

3. La Commissione incoraggia i fornitori di servizi a completare lo sviluppo dei codici di condotta entro il 29 novembre 2019 e a dare loro effettiva attuazione entro il 29 maggio 2020.

Articolo 7

Procedura di cooperazione tra le autorità

1. Ciascuno Stato membro designa un punto di contatto unico che funge da collegamento con i punti di contatto unici degli altri Stati membri e la Commissione per quanto riguarda l'applicazione del presente regolamento. Gli Stati membri comunicano alla Commissione i punti di contatto unici designati e le eventuali successive modifiche.

2. Quando l'autorità competente di uno Stato membro chiede a norma dell'articolo 5, paragrafo 2, l'assistenza di un altro Stato membro per ottenere accesso ai dati, essa inoltra una richiesta debitamente giustificata al punto di contatto unico di quest'ultimo Stato membro. Tale richiesta deve essere corredata di una illustrazione scritta dei motivi e delle basi giuridiche per accedere ai dati.

3. Il punto di contatto unico individua l'autorità competente del proprio Stato membro e le trasmette la richiesta ricevuta a norma del paragrafo 2.

4. L'autorità competente interessata che riceve la richiesta è tenuta, tempestivamente ed entro un termine proporzionato all'urgenza della richiesta, a fornire una risposta in cui comunica i dati richiesti o informa l'autorità competente richiedente che non ritiene siano state soddisfatte le condizioni per chiedere assistenza a norma del presente regolamento.

5. Tutte le informazioni scambiate nell'ambito dell'assistenza richiesta e fornita a norma dell'articolo 5, paragrafo 2, sono utilizzate solo in relazione alla questione per cui sono state richieste.

6. I punti di contatto unici forniscono agli utenti informazioni generali sul presente regolamento, anche in merito ai codici di condotta.

Articolo 8

Valutazione e orientamenti

1. Entro il 29 novembre 2022 la Commissione presenta al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo una relazione in cui valuta l'attuazione del presente regolamento, in particolare per quanto riguarda:

a) l'applicazione del presente regolamento, in particolare agli insiemi di dati composti sia da dati personali che da dati non personali, in considerazione degli sviluppi del mercato e dei progressi tecnologici suscettibili di ampliare le possibilità di de-anonimizzazione dei dati;

b) l'applicazione da parte degli Stati membri dell'articolo 4, paragrafo 1, in particolare l'eccezione relativa ai motivi di pubblica sicurezza; nonché

c) l'elaborazione e l'effettiva attuazione dei codici di condotta e l'effettiva messa a disposizione delle informazioni da parte dei fornitori di servizi.

2. Gli Stati membri forniscono alla Commissione tutte le informazioni necessarie per preparare la relazione di cui al paragrafo 1.

3. Entro il 29 maggio 2019 la Commissione pubblica orientamenti informativi sull'interazione tra il presente regolamento e il regolamento (UE) 2016/679, in particolare per quanto concerne gli insiemi di dati composti sia da dati personali che da dati non personali.

Articolo 9

Disposizioni finali

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento si applica a decorrere da sei mesi dopo la sua pubblicazione.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Strasburgo, il 14 novembre 2018

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*La presidente*
A. TAJANI	K. EDTSTADLER