

Parere del Comitato economico e sociale europeo sulla «Comunicazione della Commissione al Parlamento europeo e al Consiglio — Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea»

[COM(2019) 250 final]

(2020/C 14/18)

Relatrice: **Laure BATUT**

Consultazione	Commissione europea, 22.7.2019
Base giuridica	Articolo 304 del trattato sul funzionamento dell'Unione europea
Sezione competente	Trasporti, energia, infrastrutture, società dell'informazione
Adozione in sezione	11.9.2019
Adozione in sessione plenaria	25.9.2019
Sessione plenaria n.	546
Esito della votazione (favorevoli/contrari/astenuti)	162/2/6

1. **Raccomandazioni**

1.1. Il CESE raccomanda alla Commissione di:

- comunicare in modo semplice e chiaro quali siano i criteri per la definizione dei dati non personali e quale sia il campo di applicazione del regolamento che istituisce un quadro applicabile alla libera circolazione dei dati non personali (RDNP), al fine di dissipare le incertezze e accrescere la fiducia;
- informare gli attori del settore sugli ambiti di sovrapposizione tra i testi europei in materia di dati;
- vigilare affinché i dati personali (DP) non siano progressivamente considerati come dati non personali (DNP), pur favorendo la libera circolazione di questi ultimi, e fare in modo che il regolamento generale sulla protezione dei dati (RGPD) mantenga interamente il suo campo di applicazione, eventualmente anche unificando nel medio termine i due regolamenti in un solo testo legislativo, allo scopo di assicurare una maggiore protezione dei dati ed evitare una loro mercificazione più spinta;
- incoraggiare la creazione e lo sviluppo di federazioni di servizi paneuropei di *cloud computing*;
- aiutare nel brevissimo termine le imprese europee a utilizzare algoritmi in grado di trattare le grandi quantità di DNP nel mercato unico dei dati; incoraggiare gli Stati membri a rafforzare l'insegnamento delle tecnologie informatiche (IT) e dell'intelligenza artificiale (IA) a tutti i livelli (scuola, università, mondo del lavoro) e lungo tutto l'arco della vita;
- esortare gli attori a sviluppare uno spirito di responsabilità, etica e solidarietà, e di non permettere all'autoregolamentazione e alla composizione «amichevole» delle controversie di dare adito a interpretazioni divergenti dei testi normativi;
- non tralasciare di utilizzare lo strumento della regolamentazione;
- promuovere l'introduzione di sanzioni per le violazioni dell'autoregolamentazione;
- elaborare una tabella di marcia per verificare se la certezza del diritto sia una realtà per le imprese nel quadro del libero utilizzo dei loro dati, come previsto dall'RDNP;

- fare il punto sull'attuale situazione nei 27 Stati membri e valutare l'azione dei punti di contatto nazionali già nel loro dodicesimo mese di funzionamento;
- farsi ampiamente carico della funzione che le spetta sul piano dell'informazione, della comunicazione e della vigilanza;
- invitare gli Stati membri a comunicare con gli attori del settore in merito ai criteri di «sicurezza pubblica»;
- incoraggiare gli Stati membri a separare le aree di archiviazione dei dati non trasferibili;
- riesaminare a tempo debito la politica di concorrenza per verificare che sia adeguata alla libera circolazione dei dati nelle attuali condizioni.

2. Introduzione

2.1. Il CESE prende atto della volontà della Commissione di fornire linee guida alle imprese che partecipano al trasferimento di dati non personali prima che le parti interessate avvino, nel corso del 2020, una trattativa volta ad elaborare dei codici di condotta. Il fatto che i dati siano molto spesso «misti», cioè di natura sia personale che non personale, può creare incertezza per le imprese in rapporto alle azioni da intraprendere per proteggere tali dati. È opportuno ricordare in questa sede i principi fondamentali della regolamentazione vigente prima che vengano esaminati i punti su cui il CESE intende formulare delle osservazioni.

2.2. La Commissione ha osservato che l'assenza di competitività tra i servizi di *cloud computing* all'interno dell'UE e, di conseguenza, la mancanza di mobilità dei dati in un contesto di oligopoli hanno avuto un impatto negativo sul mercato dei dati. L'RDNP invita gli Stati membri a ridurre al minimo gli obblighi di localizzazione dei dati, nonché la frammentazione della legislazione in materia, in modo da stimolare la crescita e sbloccare le capacità di innovazione delle imprese.

2.3. Con l'adozione del regolamento sulla libera circolazione dei dati non personali, che è complementare al regolamento generale sulla protezione dei dati, viene sancita nei testi giuridici europei del XXI secolo una «quinta libertà di circolazione» (così è stata definita dalla relatrice del Parlamento europeo Anna Maria Corazza Bildt), applicabile a tutti i dati. Questa merce immateriale, se così può essere chiamata, deve poter essere trasferita e gestita, se il suo titolare lo desidera, presso prestatori di servizi di hosting di paesi diversi dallo Stato membro dell'UE in cui i dati sono stati creati e/o utilizzati (articolo 1 dell'RDNP). I titolari di questa merce ottengono pertanto dei vantaggi sul piano della semplicità e della competitività.

Il regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (RDNP)

2.4. Il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio⁽¹⁾ favorisce la libera circolazione dei dati non personali all'interno dell'Unione al fine di sviluppare l'intelligenza artificiale, il *cloud computing* e l'analisi dei megadati. Il suo articolo 6 prevede che la Commissione guidi, incoraggi e faciliti l'elaborazione, da parte degli operatori che lavorano con questi dati personali, di codici di condotta di autoregolamentazione a livello dell'Unione.

2.5. Il testo in esame, che è destinato ai professionisti delle microimprese e delle PMI, dovrebbe favorire la comprensione, da parte dei destinatari, delle interazioni esistenti tra l'RDNP e l'RGPD attraverso la presentazione di linee guida. Per assicurare la finalità pedagogica, la Commissione presenta molti esempi di situazioni.

2.6. I codici di condotta in preparazione dovrebbero essere pronti tra novembre 2019 e maggio 2020 (considerando 30 e 31, articolo 6, paragrafo 1). La loro elaborazione terrà conto del punto di vista di tutte le parti interessate. Sono state organizzate due consultazioni pubbliche, e la Commissione è coadiuvata da due gruppi di lavoro, formati da professionisti del settore: il primo si occupa della certificazione della sicurezza dei servizi *cloud* (gruppo CSPCERT), mentre il secondo si occupa della portabilità dei dati e del cambio di fornitore di servizi *cloud* (gruppo SWIPO). I loro contributi riguardano la fornitura di servizio a livello di infrastruttura (*IaaS*) e la fornitura di servizio a livello di software (*SaaS*). Nel maggio 2020 la Commissione proporrà di incoraggiare l'industria a definire un modello di clausole contrattuali e, nel 2022, riferirà al Parlamento europeo, al Consiglio e al CESE sull'applicazione del regolamento, in particolare per quanto concerne l'utilizzo di insiemi di dati compositi o misti.

3. Osservazioni generali

3.1. *Obiettivo della Commissione: conciliare il regolamento generale sulla protezione dei dati (RGPD) con il regolamento sulla libera circolazione dei dati non personali (RDNP)*

3.1.1. Al fine di conciliare i due regolamenti, che sono complementari, la Commissione spiega che: 1) gli obblighi di localizzazione dei dati **sono ormai vietati**; 2) i dati rimangono accessibili alle **autorità competenti**; 3) i dati diventano mobili e, quindi, sono portabili. La versione francese del regolamento generale sulla protezione dei dati utilizza il termine «portabilité» («portability» in inglese), mentre la versione francese del regolamento sulla libera circolazione dei dati non personali utilizza il termine «portage» («porting» in inglese) (nella versione italiana dei due regolamenti viene usato un unico termine, ossia «portabilità», N.d.T.). Gli utenti possono trasferire i loro dati al di fuori del paese in cui sono stati creati per poi recuperarli senza (troppi) vincoli dopo aver cambiato il loro fornitore di servizi per quel che riguarda l'archiviazione, il trattamento o l'analisi di tali dati. A differenza della «portabilité», che è un diritto per le persone interessate, il «portage» è basato su codici di condotta e, quindi, rientra in un approccio di autoregolamentazione.

(1) GUL 303 del 28.11.2018, pag. 59.

3.1.2. Questo aspetto rappresenta una differenza importante tra i due regolamenti, dato che il primo poggia sul **diritto cogente**, mentre il secondo è basato su strumenti non vincolanti (**soft law**), ed è risaputo che questi ultimi offrono molte meno garanzie. Secondo la stessa Commissione, la maggior parte degli insiemi di dati è formata da dati personali e non personali **indissolubilmente legati tra loro**, motivo per cui questi dati sono «misti»(DM).

3.1.3. Il CESE accoglie con favore questa impostazione di guida e sostegno, e non mette in discussione gli esempi scelti, né è sua intenzione indicarne degli altri. Osserva tuttavia che gli orientamenti della Commissione destinati agli operatori del settore si limitano a illustrare il contesto attraverso degli esempi di situazioni. Il CESE, al fine di mettere in guardia la Commissione, desidera sottolineare gli aspetti critici che, a suo avviso, sembrano porre problemi agli utenti, malgrado le linee guida pubblicate e i codici futuri.

3.2. Sintesi dei principi guida

3.2.1. Principio guida: la libera circolazione dei dati

Più che geografici, gli ostacoli alla libera circolazione dei dati non personali sono funzionali e/o connessi ai mezzi di cui dispongono le imprese per avvalersi delle tecnologie informatiche.

Il regolamento sulla libera circolazione dei dati non personali vieta gli obblighi di localizzazione di tali dati all'interno di un determinato territorio (articolo 4), e impone agli Stati membri di abrogare qualsiasi disposizione contraria entro 24 mesi dalla sua entrata in vigore (maggio 2021).

Il regolamento ammette eccezioni per motivi di pubblica sicurezza. Gli Stati devono pubblicare online informazioni dettagliate sui rispettivi obblighi di localizzazione a livello nazionale. La Commissione europea può formulare delle osservazioni e pubblica sul suo sito Internet il link che rimanda a tali informazioni.

3.2.2. Eccezioni alla libertà di circolazione

- Le autorità degli Stati membri possono avere **accesso ai dati trasferiti**: il regolamento sulla libera circolazione dei dati non personali contempla una procedura che consente a qualsiasi autorità di controllo di uno Stato X di ottenere dei dati trattati in uno Stato Y e, a tal fine, prevede una procedura di cooperazione (articoli 5 e 7). Tuttavia il CESE teme che, per effetto della mancata localizzazione, i dati (contabili, finanziari, contrattuali ecc.) sfuggano al controllo delle autorità degli Stati membri. Il Comitato ricorda alla Commissione di non tralasciare di utilizzare lo strumento della regolamentazione, ove opportuno.
- Il «**punto di contatto**»**unico** in ogni Stato membro tratterà la richiesta di accesso assieme all'autorità nazionale di controllo, che potrà fornire i dati se ritiene che la richiesta sia ammissibile. Conformemente allo spirito del regolamento, i punti di contatto dovrebbero aiutare gli attori del settore a scegliere con cognizione di causa quali dati trasferire e i fornitori di servizi cui affidarsi per il trattamento dei dati in tutta l'Unione, e questo in un regime di libera concorrenza.

Secondo il CESE, le linee guida non potranno da sole dissipare le numerose incertezze legate all'attuazione di questo principio. È difficile valutare le motivazioni degli Stati, la buona fede degli operatori o il buon funzionamento dei punti di contatto. Qualsiasi valutazione in questo campo si rivelerà complicata.

- Divieto di imporre, con mezzi diretti o indiretti, la localizzazione dei dati, tranne che per i casi giustificati di «pubblica sicurezza». Secondo il CESE, il concetto di «pubblica sicurezza» menzionato nel regolamento è impreciso, e non ne è chiaro il campo di applicazione quando riguarda il flusso di dati e la loro mercificazione. Il regolamento sulla libera circolazione dei dati non personali definisce gli obblighi di localizzazione come «qualsiasi obbligo, divieto, condizione, limite o altro requisito, previsto dalle disposizioni legislative, regolamentari o amministrative di uno Stato membro», oppure risultante dalle prassi amministrative^(?), che imporrebbe agli operatori di conservare i dati entro i confini di un dato territorio all'interno dell'Unione. Per la Corte di giustizia dell'Unione europea (CGUE)^(?) (come ricordato nel considerando 19 del regolamento), la nozione di pubblica sicurezza riguarda «la sicurezza sia interna che esterna di uno Stato membro» e presuppone «l'esistenza di una minaccia reale e sufficientemente grave a uno degli interessi fondamentali della società». Questa definizione comprende i dati genetici, biometrici e sanitari. La risposta dello Stato membro deve essere proporzionata.

^(?) Regolamento (UE) 2018/1807, articolo 3, paragrafo 5.

^(?) Cfr. la comunicazione COM(2019) 250, note in calce a pag. 13 e cause riunite C-331/16 e C-366/16, *K. contro Staatssecretaris van Veiligheid en Justitie e H.F. contro Belgische Staat*: «42. Quanto alla **nozione di «pubblica sicurezza»**, dalla giurisprudenza della Corte risulta che tale nozione **comprende tanto la sicurezza interna di uno Stato membro** quanto la sua sicurezza esterna (sentenza del 23 novembre 2010, *Tsakouridis*, C-145/09, EU:C:2010:708, punto 43). La sicurezza interna può essere pregiudicata, in particolare, da una **minaccia diretta per la tranquillità e la sicurezza fisica** della popolazione dello Stato membro interessato (v., in tal senso, sentenza del 22 maggio 2012, *I.*, C-348/09, EU:C:2012:300, punto 28). Quanto alla sicurezza esterna, essa può essere pregiudicata, in particolare, dal **rischio di perturbazioni gravi dei rapporti internazionali di tale Stato membro** o della coesistenza pacifica dei popoli (v., in tal senso, sentenza del 23 novembre 2010, *Tsakouridis*, C-145/09, EU:C:2010:708, punto 44)».

3.2.3. Secondo il Comitato, per quanto concerne sia la libera circolazione dei dati che la loro localizzazione:

- i criteri selezionati possono essere oggetto di molteplici interpretazioni;
- soltanto il giudice potrà chiarire, caso per caso, l'interpretazione da dare, e questo potrebbe intaccare la fiducia che è indispensabile negli scambi commerciali, in particolare per i dati sensibili. Le controversie sorte per effetto dei codici di condotta potrebbero accrescere la frammentazione delle situazioni;
- la giustizia ha i suoi tempi, che sono ben diversi da quelli del mondo digitale e del trasferimento dei dati.

Il CESE ritiene che le incertezze e la complessità della situazione costituiscano un disincentivo per le microimprese e le PMI.

3.2.4. Il CESE deplora che le linee guida non facciano alcun riferimento alle controversie o alle modalità per verificare in che modo gli Stati membri rispetteranno i criteri della pubblica sicurezza, né ad eventuali sanzioni nei loro confronti, ove opportuno. Il CESE teme che le spiegazioni racchiuse nella comunicazione non siano sufficienti a permettere agli operatori delle microimprese e delle PMI di trovare la giusta rotta tra gli scogli giuridici dei testi. Teme altresì che tali incertezze non consentano di infondere il sentimento di fiducia e di certezza giuridica che è necessario per lo sviluppo del settore.

3.2.5. Il CESE riconosce che la comunicazione della Commissione ha il grande merito di dare ampia diffusione, secondo un approccio dall'alto, a informazioni riguardanti la situazione creata dai due regolamenti. Tale comunicazione è quanto mai necessaria per il mondo delle microimprese e delle PMI. Il CESE auspica che l'azione dei punti di contatto nazionali e l'utilizzo del sito web della Commissione da parte di questi attori siano oggetto di valutazione a partire dal sesto mese di funzionamento, ai fini di una rapida applicazione di eventuali misure correttive qualora venisse riscontrata una carenza di informazione e comunicazione.

4. Osservazioni particolari

4.1. I dati

4.1.1. I dati non personali comprendono, per definizione, tutti i dati digitali che non rientrano nel concetto di dato personale così come definito dal regolamento generale sulla protezione dei dati. Può trattarsi di dati commerciali, di dati sull'agricoltura di precisione, sulle esigenze di manutenzione delle macchine, sulle condizioni meteorologiche ecc.

4.1.2. È possibile che i dati raccolti da servizi pubblici come gli ospedali, o quelli connessi all'assistenza sociale o all'amministrazione fiscale, si trovino in totale contiguità con i dati personali dei pazienti o dei contribuenti. Le imprese che potrebbero utilizzarli devono vigilare affinché tali dati non consentano di identificare delle persone, e garantire che il loro processo di anonimizzazione, una volta effettuato, non possa essere invertito. Per una microimpresa o una PMI questo potrebbe comportare il ricorso a procedure troppo dispendiose in termini di tempo e denaro. Poiché i due regolamenti (RGPD e RDNP) garantiscono insieme la libera circolazione di tutti i dati nell'UE, quando tali dati sono «**indissolubilmente legati**», le tutele giuridiche previste nel regolamento generale sulla protezione dei dati sono applicabili anche agli insiemi di dati misti (considerando 8 e articolo 2, paragrafo 2, del regolamento (UE) 2018/1807). Alla prima restrizione alla libera circolazione dei dati non personali, che è connessa a motivi di pubblica sicurezza, si aggiunge quindi una seconda restrizione, legata alla natura stessa dei dati. È questo il punto centrale della comunicazione della Commissione, che fa più volte riferimento alla contiguità tra dati personali e non personali: «gli insiemi di dati misti rappresentano la maggior parte degli insiemi di dati»(comunicazione, punto 2.2); questi dati possono essere «indissolubilmente legati»(punto 2.2); «nessuno dei due regolamenti impone alle imprese di separare gli insiemi di dati»(punto 2.2).

4.1.3. Spetta all'impresa chiedersi se i dati non personali oggetto di trattamento siano «indissolubilmente legati» a dei dati personali e, in caso affermativo, proteggerli. Per l'impresa, non è semplice mettere in atto una gestione esterna dei dati (*out management*). Non sembra possibile giungere ad una definizione generale dei dati misti, e la sovrapposizione tra i due regolamenti comporta probabilmente a sua volta una sovrapposizione con altri testi relativi alla legislazione in materia di dati, come quelli riguardanti la proprietà intellettuale: i dati non personali possono circolare, ma non saranno più soggetti alle stesse norme se vengono riutilizzati all'interno di un'opera. Il CESE prevede che le interazioni tra i vari testi saranno molto delicate. La giurisprudenza ha già stabilito che l'indissolubilità del legame deve essere esaminata secondo un criterio di ragionevolezza. Secondo il CESE, la comunicazione non è manifestamente in grado di passare in rassegna tutte le fattispecie al fine di aiutare gli attori del settore, e la situazione creata favorisce prevalentemente le grandi imprese. Il CESE raccomanda alla Commissione di vigilare affinché, nella pratica, i dati personali non siano progressivamente considerati come dati non personali, e di fare in modo che il regolamento generale sulla protezione dei dati mantenga integralmente il suo campo di applicazione, eventualmente anche unificando, nel medio termine, i due regolamenti in un solo testo legislativo, allo scopo di assicurare una maggiore protezione dei dati ed evitare una loro mercificazione più spinta.

4.2. La portabilità, il trasferimento, il trattamento e l'archiviazione dei dati

Il regolamento generale sulla protezione dei dati prevede che la portabilità debba essere disciplinata tramite una regolamentazione (articolo 20), mentre il regolamento sulla libera circolazione dei dati non personali punta sull'autoregolamentazione. Il CESE teme che questa differenza possa dare adito a una notevole incertezza giuridica, che rischia di penalizzare le microimprese e le PMI a causa dei molteplici rischi di contenzioso. Secondo il CESE, è possibile importare ed esportare i dati non personali, se questi sono una merce (seppure immateriale) in libera circolazione. Nell'attuale contesto sarebbe interessante tenere un dibattito sulla loro proprietà. Tuttavia, il valore commerciale di tali «merci» non risiede nei dati presi singolarmente, ma nella loro massa. Questa considerazione spinge il Comitato a ritenere che la politica in materia di concorrenza potrebbe non essere adeguata a questo tipo di mercato. Il CESE si chiede in che modo la situazione creata rafforzi la produttività delle microimprese e delle PMI, ma su questo punto la comunicazione della Commissione non offre alcuna chiave di lettura.

4.3. I fornitori di servizi

4.3.1. L'UE non dispone di grandi operatori, né di un *cloud* «europeo», una situazione che il CESE deplora da lungo tempo. L'effetto scala sempre ricercato è una prerogativa dei giganti dell'informatica statunitensi e di talune imprese cinesi. Per questo motivo, persino le amministrazioni pubbliche degli Stati membri tendono a fare assegnamento su queste imprese e a demandare loro la gestione dei dati (è il caso della Francia).

4.3.2. Secondo il CESE, gli europei avrebbero bisogno di creare ecosistemi partner e di prevedere i trasferimenti interpiattaforma dei dati. Al di là delle linee guida formulate nella comunicazione in esame, la Commissione potrebbe aiutare le microimprese e le PMI a sviluppare delle risorse a questo scopo, come ha fatto per i servizi di interesse generale (SIG) nel suo progetto del 2018 relativo a una federazione di servizi paneuropei di *cloud computing* per la prestazione di servizi economici e non economici d'interesse generale (servizio a livello di funzione o *FaaS*) e come ha previsto con la rete di poli dell'innovazione digitale (A network of Digital Innovation Hubs (DIH), [web/Commissione/DIH/gennaio 2019](http://web/Commissione/DIH/gennaio%202019)).

4.4. La sicurezza dei dati ⁽⁴⁾

4.4.1. A livello interno, gli operatori nazionali ⁽⁵⁾ verificano la natura dei dati da trasferire e ne garantiscono la sicurezza. L'obbligo di localizzazione trovava il suo fondamento in regole di sicurezza controllabili conformemente al diritto nazionale. Tuttavia, le norme in materia di sicurezza informatica, malgrado l'adozione dei regolamenti RGPD e RDNP, non sono unificate tra i diversi Stati membri dell'UE. Secondo il CESE, bisognerebbe fornire informazioni molto rigorose su questo punto alle microimprese e alle PMI, oltre che ai servizi pubblici e privati, per il tramite dei punti di contatto nazionali e in diverse lingue.

A livello esterno, il CESE ritiene che non esista certezza in merito alla capacità delle imprese esterne all'UE di rispettare i codici di condotta e di restituire i dati dopo eventuali ulteriori trasferimenti richiesti dai loro titolari. Il Comitato teme che, nel lungo termine, diventi difficile dipanare le responsabilità.

Il CESE raccomanda alla Commissione di aiutare gli attori europei del settore affinché riescano nel brevissimo termine ad utilizzare algoritmi in grado di gestire le grandi quantità di dati non personali trattate nel mercato unico dei dati.

4.4.2. La questione riguardante l'ubicazione fisica dei server e la loro sicurezza rimarrà un aspetto delle trattative commerciali e diplomatiche tra Stato e Stato. Tale questione è fondamentale. Tenuto conto del peso dei giganti dell'informatica e del rispettivo Stato di riferimento, per gli Stati membri condurre delle trattative per conto proprio non sarebbe esente da rischi, anche se la gestione dei dati è una competenza condivisa tra gli Stati membri e l'UE.

4.4.3. Il CESE propone alla Commissione di chiarire la comunicazione per quanto riguarda gli obblighi dei fornitori di servizi in materia di archiviazione dei dati non personali, i metodi utilizzati, la localizzazione concreta, la durata di conservazione prevista o autorizzata e l'utilizzo dopo il trattamento, dato che questi elementi condizionano la sicurezza dei dati e possono rivestire importanza per le imprese europee nel contesto della concorrenza mondiale.

4.5. I codici di condotta

4.5.1. A partire da maggio 2019, gli attori del settore che sono i destinatari del regolamento sulla libera circolazione dei dati non personali (principalmente, utenti e fornitori di servizi *cloud*) sono incoraggiati a elaborare il proprio codice di condotta entro un termine di 12 mesi. Secondo la Commissione, è opportuno tener conto delle migliori prassi in questo settore, degli approcci relativi ai sistemi di certificazione e delle tabelle di marcia in materia di comunicazione. I gruppi di lavoro SWIPO e CSPCERT apportano le loro competenze specialistiche.

4.5.2. La Commissione fa riferimento a quanto è stato fatto per il regolamento generale sulla protezione dei dati (come indicato alla pag. 23 della comunicazione in esame). Infatti questo regolamento, poiché segue l'orientamento del Garante europeo della protezione dei dati (GEPD) ⁽⁶⁾, può essere utilizzato come base di riferimento per il regolamento sulla libera circolazione dei dati non personali. Il codice di condotta può essere elaborato da associazioni di categoria. Gli autori del codice devono dimostrare alle autorità competenti che il testo da loro elaborato, applicabile a livello nazionale o transnazionale, soddisfa una necessità specifica del settore, facilita l'applicazione del regolamento e introduce meccanismi efficaci per il controllo del rispetto del codice.

⁽⁴⁾ GU C 227 del 28.6.2018, pag. 86.

⁽⁵⁾ GU C 218 del 23.7.2011, pag. 130.

⁽⁶⁾ GEPD, Comitato europeo per la protezione dei dati: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies*, 12.2.19, https://edpb.europa.eu/our-work-tools/our-documents/guidelines-12019-codes-conduct-and-monitoring-bodies-under_it

4.5.3. Anche prima dell'entrata in vigore del regolamento generale sulla protezione dei dati, i principali fornitori di servizi a livello di infrastrutture (*IaaS*) e a livello di software (*SaaS*) avevano sviluppato un loro codice di condotta volto a definire le modalità del loro operato e, quindi, a dissipare le incertezze messe in luce dai professionisti del settore ⁽⁷⁾. I fornitori di servizi avevano coinvolto le PMI, ritenendo che per molte di queste imprese l'autocertificazione fosse preferibile al costo molto elevato di una certificazione.

4.5.4. Il CESE appoggia un approccio settoriale per il regolamento sulla libera circolazione dei dati non personali, qualora non risulti appropriata una soluzione unica valida per tutti. Nel quadro del regolamento generale sulla protezione dei dati (articolo 40, paragrafo 2) è stato stilato un elenco non esaustivo degli elementi che i codici di condotta devono prendere in considerazione, in particolare per quanto riguarda il trattamento corretto e trasparente dei dati, la sicurezza nel trasferimento dei dati e la risoluzione delle controversie. Gli attori del settore vanno esortati, nel loro stesso interesse e al fine di rafforzare la fiducia dei consumatori nell'approccio europeo, a ispirarsi a tali principi e a sviluppare uno spirito di responsabilità, etica e solidarietà, in particolare tramite orientamenti che tengano conto dell'intelligenza artificiale. Si tratta di uno dei punti su cui il CESE intende richiamare l'attenzione, e raccomanda pertanto alla Commissione di non permettere all'autoregolamentazione e alla composizione «amichevole» delle controversie di dare adito a interpretazioni divergenti dei testi normativi. Sarebbe invece opportuno fare tutto il possibile per amalgamarli in unico testo, per poi trasformare le relative disposizioni in regole applicabili a tutti e annunciare tale unificazione nelle tabelle di marcia sull'informazione e la comunicazione.

5. La valutazione

La Commissione procederà a una valutazione periodica per quanto concerne l'impatto sulla libera circolazione dei dati, l'applicazione del regolamento, l'abrogazione delle misure restrittive da parte degli Stati membri e l'efficacia dei codici di condotta. Secondo il CESE, in tale contesto i rappresentanti della società civile dovrebbero essere invitati ad esprimere il loro punto di vista ⁽⁸⁾. Perché la società nel suo complesso nutra un sentimento di sicurezza e, di conseguenza, abbia fiducia nelle nuove prassi digitali, tanto l'Unione quanto gli Stati membri devono dissipare ogni incertezza per quel che riguarda il diritto applicabile, la riservatezza, la conservazione e il recupero senza perdite dei dati, le garanzie di fattibilità e la buona fede degli attori, nonché le garanzie finanziarie. L'indissolubilità dei dati che sono al tempo stesso personali e non personali è fonte d'inquietudine, e la percentuale di questo tipo di dati rispetto all'insieme di tutti i dati spinge il CESE a chiedersi se l'autoregolamentazione rappresenti realmente l'unica soluzione possibile. Il CESE raccomanda che, nel medio termine, le norme del regolamento generale sulla protezione dei dati siano applicabili a tutti i dati e ai loro trasferimenti, e che siano previste delle eccezioni per i «veri» dati non personali.

Bruxelles, 25 settembre 2019

Il presidente
del Comitato economico e sociale europeo
Luca JAHIER

⁽⁷⁾ CISPE (Fornitori di servizi di infrastrutture cloud in Europa).

⁽⁸⁾ GU C 487 del 28.12.2016, pag. 92 e GU C 62 del 15.2.2019, pag. 292.

ALLEGATO

I seguenti emendamenti sono stati respinti, ma hanno ottenuto almeno un quarto dei voti espressi (articolo 59, paragrafo 3 del Regolamento interno):

Punto 4.1.3

Modificare come segue:

Spetta all'impresa chiedersi se i dati non personali oggetto di trattamento siano «indissolubilmente legati» a dei dati personali e, in caso affermativo, proteggerli. Per l'impresa, non è semplice mettere in atto una gestione esterna dei dati (out management). Non sembra possibile giungere ad una definizione generale dei dati misti, e la sovrapposizione tra i due regolamenti comporta probabilmente a sua volta una sovrapposizione con altri testi relativi alla legislazione in materia di dati, come quelli riguardanti la proprietà intellettuale: i dati non personali possono circolare, ma non saranno più soggetti alle stesse norme se vengono riutilizzati all'interno di un'opera. Il CESE prevede che le interazioni tra i vari testi saranno molto delicate. La giurisprudenza ha già stabilito che l'indissolubilità del legame deve essere esaminata secondo un criterio di ragionevolezza. Secondo il CESE, la comunicazione non è manifestamente in grado di passare in rassegna tutte le fattispecie al fine di aiutare gli attori del settore, e la situazione creata favorisce prevalentemente le grandi imprese. Il CESE raccomanda alla Commissione di vigilare affinché, nella pratica, i dati personali non siano progressivamente considerati come dati non personali, e di fare in modo che il regolamento generale sulla protezione dei dati mantenga integralmente il suo campo di applicazione, eventualmente anche unificando, nel medio termine, i due regolamenti in un solo testo legislativo, allo scopo di assicurare una maggiore protezione dei dati ed evitare una loro mercificazione più spinta.

Punto 5

Modificare come segue:

La Commissione procederà a una valutazione periodica per quanto concerne l'impatto sulla libera circolazione dei dati, l'applicazione del regolamento, l'abrogazione delle misure restrittive da parte degli Stati membri e l'efficacia dei codici di condotta. Secondo il CESE, in tale contesto i rappresentanti della società civile dovrebbero essere invitati ad esprimere il loro punto di vista. Perché la società nel suo complesso nutra un sentimento di sicurezza e, di conseguenza, abbia fiducia nelle nuove prassi digitali, tanto l'Unione quanto gli Stati membri devono dissipare ogni incertezza per quel che riguarda il diritto applicabile, la riservatezza, la conservazione e il recupero senza perdite dei dati, le garanzie di fattibilità e la buona fede degli attori, nonché le garanzie finanziarie. L'indissolubilità dei dati che sono al tempo stesso personali e non personali è fonte d'inquietudine, e la percentuale di questo tipo di dati rispetto all'insieme di tutti i dati spinge il CESE a chiedersi se l'autoregolamentazione rappresenti realmente l'unica soluzione possibile. Il CESE raccomanda che, nel medio termine, le norme del regolamento generale sulla protezione dei dati siano applicabili a tutti i dati e ai loro trasferimenti, e che siano previste delle eccezioni per i «veri» dati non personali.

Punto 1.1, terzo punto in neretto

Modificare come segue:

Il CESE raccomanda alla Commissione di:

...

- *vigilare affinché i dati personali (DP) non siano progressivamente considerati come dati non personali (DNP), pur favorendo la libera circolazione di questi ultimi, e fare in modo che il regolamento generale sulla protezione dei dati (RGPD) mantenga interamente il suo campo di applicazione, eventualmente anche unificando nel medio termine i due regolamenti in un solo testo legislativo, allo scopo di assicurare una maggiore protezione dei dati ed evitare una loro mercificazione più spinta;*

...

Motivazione

Il regolamento generale sulla protezione dei dati e il regolamento (UE) 2018/1807 hanno basi giuridiche diverse, rispettivamente l'articolo 16 del TFUE, relativo al diritto fondamentale degli individui alla protezione dei dati personali, e l'articolo 114 del TFUE, sul ravvicinamento delle disposizioni legislative. Tale distinzione consente all'UE di disporre di un margine di intervento diverso nei confronti delle imprese private (ragione per cui nel primo caso l'UE è intervenuta con una regolamentazione molto rigorosa e dettagliata, mentre nel secondo caso ha scelto l'autoregolamentazione in quanto strumento più adeguato e proporzionale di intervento). Pertanto, i due strumenti non possono essere unificati sul piano giuridico.

Esito della votazione dell'emendamento

Voti favorevoli:	54
Voti contrari:	84
Astensioni:	18