Parlamento europeo
2019-2024

Commissione per le libertà civili, la giustizia e gli affari interni

2020/2217(INI)

17.2.2021

PARERE

della commissione per le libertà civili, la giustizia e gli affari interni

destinato alla commissione per l'industria, la ricerca e l'energia

su una strategia europea per i dati
(2020/2217(INI))

Relatrice per parere: Marina Kaljurand

(*) Procedura con le commissioni associate – articolo 57 del regolamento

PA_NonLeg

SUGGERIMENTI

La commissione per le libertà civili, la giustizia e gli affari interni invita la commissione per l'industria, la ricerca e l'energia, competente per il merito, a includere nella proposta di risoluzione che approverà i seguenti suggerimenti:

– vista la Carta dei diritti fondamentali dell'Unione europea ("la Carta"),

– visto il 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 (GDPR)[1],

– vista la 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 (direttiva sull'applicazione della legge, LED)[2],

– vista la direttiva 2002/58/CE del Parlamento Europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva e-privacy)[3],

– visto il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea[4],

– vista la direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (direttiva sull'apertura dei dati)[5],

A. considerando che l'articolo 8, paragrafo 1, della Carta e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE) stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

B. considerando che la Carta stabilisce che ogni individuo ha diritto alla libertà di espressione, che include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera;

Principi generali della governance dei dati

1. invita la Commissione a basare la sua strategia per i dati sui principi volti a conferire

[1] GU L 119 del 4.5.2016, pag. 1.
[2] GU L 119 del 4.5.2016, pag. 89.
[3] GU L 201 del 31.7.2002, pag. 37.
[4] GU L 303 del 28.11.2018, pag. 59.
[5] GU L 172 del 26.6.2019, pag. 56.

benessere ai cittadini, dando loro il potere di assumere decisioni importanti sui dati che hanno prodotto o che li riguardano, ponendo al centro dell'ambiente politico gli interessi e i diritti degli individui, in particolare il rispetto della dignità e dell'integrità umana, e la protezione della vita privata e dei dati personali; esorta pertanto la Commissione a essere estremamente vigile nella sua progettazione delle strutture di governance dei dati e di accesso ai dati per l'Europa; chiede che il comitato europeo per l'innovazione in materia di dati sia composto in egual misura da rappresentanti dell'industria, delle ONG, dei gruppi di consumatori e del mondo accademico;

2. sottolinea, in particolare nel contesto dei flussi di dati, che i trasferimenti di dati personali verso altre giurisdizioni devono sempre rispettare le disposizioni del GDPR o della direttiva LED, della Carta e di altre normative pertinenti dell'Unione, e tener conto delle raccomandazioni e degli orientamenti del comitato europeo per la protezione dei dati (EDPB) prima di qualsiasi trasferimento, e che tali trasferimenti possono aver luogo solo se vi è un livello sufficiente di protezione dei dati personali; invita la Commissione a proseguire gli sforzi volti a garantire flussi di dati sicuri con partner globali accomunati dagli stessi principi, sulla base di valori condivisi e del pieno rispetto dei diritti fondamentali; esprime il suo orgoglio per il fatto che l'UE ha assunto una posizione ferma adottando il GDPR e potenziando le norme in materia di protezione dei dati che rafforzano i diritti fondamentali;

3. sottolinea che i dati personali sono generati a ritmi esponenziali e pone l'accento sul valore economico dei dati personali che è importante per la crescita e lo sviluppo; ricorda che il trattamento dei dati personali, compreso il loro trasferimento, deve sempre essere conforme all'acquis dell'Unione in materia di protezione dei dati, che deve essere rispettato da qualsiasi futura normativa settoriale o ad hoc; evidenzia, a tale proposito, la necessità di distinguere chiaramente tra il trattamento dei dati personali e non personali negli spazi di dati delineati dalla Commissione, in particolare nel caso dei prodotti connessi intelligenti e di dispositivi indossabili; osserva che tale distinzione può essere difficile da tracciare nella pratica in ragione dell'esistenza di insiemi di dati misti; ricorda, in tale contesto, che gli insiemi di dati in cui sono indissolubilmente collegati diversi tipi di dati sono sempre trattati come dati personali, anche nei casi in cui i dati personali rappresentano solo una piccola parte dell'insieme di dati; ritiene che dovrebbero essere forniti orientamenti molto più chiari alle imprese sull'utilizzo di set di dati misti e che dovrebbe essere incoraggiato l'uso di tecnologie a tutela della vita privata per aumentare la certezza del diritto per le imprese, tra l'altro attraverso orientamenti chiari e un elenco di criteri per un'efficace anonimizzazione; sottolinea che il controllo di tali dati spetta sempre all'individuo e dovrebbe essere automaticamente protetto; invita la Commissione ad ampliare la sua strategia in materia di dati in modo da garantire che i cittadini abbiano la capacità e la facoltà di trarre vantaggio dai propri dati personali;

4. mette in guardia contro il rischio di un uso improprio dei dati personali o del contenuto e dei metadati delle comunicazioni elettroniche nell'ambito di applicazione della direttiva e-privacy; sottolinea che, in conformità del principio di limitazione della finalità sancito dal GDPR, la libera condivisione dei dati deve essere limitata ai dati non personali, ad esempio i dati industriali o commerciali, ovvero ai dati personali resi anonimi in modo sicuro, efficace e irreversibile anche nel caso degli insiemi di dati misti; invita la Commissione a tenere conto dei minori nella sua strategia in materia di

dati;

5. rileva come le pratiche di condivisione, gli ecosistemi e il trattamento dei dati irresponsabili, illegali o non etici incoraggino i comportamenti problematici; esprime preoccupazione riguardo alla proliferazione di tali pratiche ed evidenzia quanto questi tipi di modelli economici possano avere ripercussioni molto intrusive e negative, non soltanto sulle persone e sui loro diritti fondamentali, ma anche sulle società nel loro complesso; sottolinea che tali pratiche e strategie possono compromettere la fiducia dei cittadini nei sistemi di dati dell'UE; invita pertanto la Commissione a provvedere affinché il ruolo di primo piano che l'UE è destinata a conseguire nell'ambito dell'economia dei dati sia fondato sulle solide basi giuridiche stabilite dall'acquis dell'Unione in materia di protezione dei dati;

6. invita la Commissione a garantire che i concetti di "riutilizzo dei dati" e "altruismo dei dati" siano conformi ai principi in materia di protezione dei dati, in particolare la limitazione delle finalità, che impone che i dati siano trattati per "finalità determinate, esplicite e legittime";

7. pone l'accento sulla crescente importanza delle attività di controllo esercitate dalle autorità nazionali garanti della protezione dei dati e chiede agli Stati membri di assicurare loro piena indipendenza e adeguati finanziamenti e risorse; ricorda che qualsiasi misura da mettere a punto nel proposto atto sulla governance dei dati e in altre proposte future che comportino il trattamento di dati personali è soggetta al controllo delle autorità garanti della protezione dei dati a norma del GDPR al fine di garantire che l'innovazione tenga conto anche dell'impatto sui diritti dei cittadini; chiede che gli atti si basino sulla legislazione vigente e siano allineati con essa, in particolare il GDPR;

8. invita la Commissione a utilizzare appieno i finanziamenti dell'Unione destinati allo sviluppo di prodotti e servizi per la tutela della vita privata nell'UE, affinché la strategia per i dati offra vantaggi ai cittadini dell'Unione e incoraggi un'innovazione volta a rispettare e promuovere i diritti fondamentali;

9. pone in particolare l'accento sull'importanza dei dati non personali detenuti e prodotti dalle amministrazioni e dal settore pubblico; invita gli Stati membri a promuovere la creazione di dati non personali basati sul principio dell'"apertura fin dalla progettazione e per impostazione predefinita", allo scopo di agevolare l'accesso alle informazioni del settore pubblico e il loro riutilizzo;

Spazi di dati

10. sottolinea che sarà possibile conquistare la fiducia dei cittadini solo attraverso spazi di dati sicuri e protetti che rispettino pienamente i diritti fondamentali, garantendo in tal modo la certezza giuridica, la diffusione di servizi, nonché vantaggi competitivi e modelli economici stabili per le aziende; sottolinea che tali spazi di dati dovrebbero sviluppati, creati e utilizzati in linea con i principi della protezione dei dati "fin dalla progettazione" e "per impostazione predefinita" e dovrebbero attuare rigorose misure di sicurezza;

11. sottolinea che gli spazi comuni europei di dati per le pubbliche amministrazioni, in particolare per quanto concerne l'uso dei dati per migliorare l'accesso ai dati da parte

delle autorità di contrasto nell'UE, devono rispettare appieno il diritto dell'Unione, compresi i principi di necessità e di proporzionalità e le norme in materia di protezione della vita privata e dei dati personali, la presunzione di innocenza e le norme procedurali; pone l'accento sulle potenzialità di migliorare la qualità dell'applicazione della legge e di combattere i condizionamenti, laddove esistono, raccogliendo dati affidabili e rendendoli accessibili al pubblico, alla società civile e agli esperti indipendenti; ricorda che qualsiasi accesso da parte delle autorità di contrasto ai dati personali pubblici o privati presenti negli spazi di dati deve essere basato sulla legislazione dell'UE e degli Stati membri, essere strettamente limitato a quanto necessario e proporzionato ed essere accompagnato da adeguate garanzie; sottolinea che l'uso dei dati personali e dell'intelligenza artificiale da parte delle autorità pubbliche dovrebbe essere consentito soltanto in presenza di un rigoroso controllo democratico e di ulteriori garanzie contro il loro uso improprio;

12. ricorda che, a prescindere dal fatto che siano considerati insiemi di dati di elevato valore, il trattamento di categorie particolari di dati personali ai sensi dell'articolo 9 del RGPD (quali dati biometrici, genetici e sanitari), anche nel contesto dello spazio comune europeo dei dati sanitari, è in linea di principio vietato, con alcune rigorose eccezioni, che comportano norme specifiche in materia di trattamento e prevedono sempre l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati; evidenzia le conseguenze potenzialmente disastrose e irreversibili per gli interessati derivanti da un trattamento illecito o non sicuro di dati sensibili; ricorda che gli insiemi di dati possono riproporre e rafforzare i condizionamenti esistenti all'interno della società; mette in guardia contro le possibilità di discriminazione e di abuso;

13. osserva che la soluzione più efficiente per ridurre i condizionamenti nei sistemi ricchi di dati consiste nel garantire la massima disponibilità possibile di dati non personali per addestrare tali sistemi, il che impone di limitare gli ostacoli inutili all'estrazione di testo e di dati e di agevolarne l'uso transfrontaliero; chiede che siano sfruttate al meglio le eccezioni e le deroghe esistenti previste dalla legge nell'utilizzo dei dati protetti dai diritti di proprietà intellettuale, al fine di rendere l'IA e l'apprendimento automatico meno soggetti a condizionamenti e più in linea con le norme etiche, con l'obiettivo finale di servire meglio l'umanità;

Diritti in materia di dati – conferire responsabilità all'individuo

14. pone l'accento sulle limitazioni poste a talune tipologie di applicazioni di IA destinate alla magistratura, le cosiddette applicazioni "legal tech"; evidenzia, in tale contesto, le ripercussioni negative potenzialmente gravi, in particolare nel settore delle attività di contrasto e della giustizia, qualora le persone non tengano conto della possibilità che i risultati basati sull'IA siano errati, incompleti, non pertinenti o discriminatori; ricorda che le decisioni giudiziarie definitive devono essere a discrezione dei giudici, caso per caso; osserva che gli scambi di dati tra gli Stati membri nei settori della giustizia e degli affari interni sono importanti ai fini del rafforzamento della sicurezza dei cittadini europei e che dovrebbero essere stanziate adeguate risorse finanziarie a tale riguardo; sottolinea, tuttavia, che sono necessarie maggiori garanzie per quanto riguarda il modo in cui le agenzie della giustizia e degli affari interni trattano, utilizzano e gestiscono le informazioni personali e i dati negli spazi di dati proposti;

15. sottolinea l'asimmetria tra coloro che impiegano le tecnologie di intelligenza artificiale e coloro che interagiscono con tali tecnologie e sono soggetti ad esse; esprime preoccupazione per le piattaforme e i servizi che immobilizzano i loro utenti su una determinata piattaforma, amplificando in tal modo il loro potere dominante di mercato e la loro capacità di profilare i propri utenti, creandone profili estremamente invasivi dei loro utenti; evidenzia che le competenze tecniche di cui dispone la stragrande maggioranza dei cittadini, necessarie a comprendere e gestire la complessità degli ecosistemi di dati che li riguardano, sono insufficienti, proprio come la loro capacità di individuare quali dati e metadati realmente generano, soprattutto in tempo reale, ad esempio attraverso l'uso di dispositivi connessi e indossabili;

16. sottolinea che i cittadini dovrebbero avere pieno controllo dei loro dati e beneficiare di ulteriore assistenza nel far valere i loro diritti in materia di protezione dei dati e della vita privata, con riferimento ai dati che generano; pone l'accento sul diritto alla portabilità dei dati e sui diritti della persona interessata previsti dal GDPR in materia di accesso, rettifica e cancellazione; invita la Commissione e gli Stati membri a migliorare ulteriormente l'accesso delle persone a mezzi di ricorso efficaci a norma del GDPR e a garantire l'interoperabilità e la portabilità dei dati dei servizi digitali e, in particolare mediante interfacce per programmi applicativi , consentendo a un utente di interconnettersi tra le piattaforme e aumentando le possibilità di scelta tra diversi tipi di sistemi e servizi; si attende che le future proposte sostengano il godimento e l'esercizio significativo di tali diritti;

17. è del parere che esistano grandi potenzialità in termini di utilizzo dei dati a fini di ricerca nell'interesse pubblico; chiede un'efficace anonimizzazione e sottolinea che, laddove uno scopo di ricerca non consenta l'anonimizzazione, dovrebbe essere utilizzata la pseudonimizzazione; sottolinea che gli interessati non dovrebbero subire pressioni a condividere i loro dati e che tale decisione non deve essere legata a vantaggi diretti per coloro che scelgono di esprimere il consenso all'utilizzo dei propri dati personali;

18. sottolinea inoltre che qualsiasi utilizzo di dati personali aggregati provenienti dai social media deve essere conforme al GDPR oppure subire un processo di anonimizzazione realmente irreversibile; chiede alla Commissione di promuovere le migliori pratiche in materia di tecniche di anonimizzazione e di stimolare ulteriormente la ricerca sul processo di inversione dell'anonimizzazione e sui modi per contrastarla; invita la EDPB ad aggiornare i propri orientamenti al riguardo; esprime tuttavia cautela circa il ricorso all'anonimizzazione come tecnica per tutelare la vita privata, dato che in alcuni casi è praticamente impossibile ottenere un'anonimizzazione completa;

Sicurezza informatica e informazioni sicure

19. sottolinea l'importanza della sicurezza informatica e della resilienza dei sistemi informatici, per garantire la sicurezza dei dati personali e impedire l'uso improprio dei dati; sottolinea l'importanza della cibersicurezza basata sul diritto dell'UE e internazionale e sulle norme concordate per un comportamento responsabile degli Stati nel ciberspazio; invita gli Stati membri, insieme all'Agenzia dell'Unione europea per la cibersicurezza, recentemente rafforzata, ad adottare un'azione coordinata; invita la Commissione a proporre adeguate misure cautelative, quali l'obbligo di utilizzare la sicurezza informatica e la crittografia più avanzate, l'uso di un approccio alla "sicurezza

fin dalla progettazione" e un forte programma di certificazione informatica attraverso il quadro di certificazione informatica dell'UE per aumentare la fiducia nella sicurezza degli spazi di dati;

20. accoglie con favore le conclusioni del Consiglio dell'ottobre 2020 sullo sviluppo di un quadro a livello UE per l'identificazione elettronica (e-ID) pubblica e sicura; è fermamente convinto che un quadro di identificazione elettronica affidabile sia fondamentale per garantire un accesso sicuro ai servizi digitali pubblici, per effettuare transazioni elettroniche in modo più sicuro e per ridurre la raccolta eccessiva di dati da parte delle imprese; osserva che attualmente solo 15 Stati membri hanno notificato un regime di identità elettronica per il riconoscimento transfrontaliero nel quadro del regolamento (UE) n. 910/2014 ("regolamento eIDAS")[6]; invita la Commissione ad ampliare il quadro per la sicurezza dell'identificazione elettronica pubblica al fine di fornire ai cittadini europei gli strumenti adeguati per poter accedere ai servizi laddove sia necessaria un'identificazione univoca; ricorda, a tale proposito, l'importanza di consentire, nei limiti del possibile, l'anonimato nell'utilizzo dei servizi online; ritiene che la legislazione non dovrebbe richiedere inutilmente l'identificazione, in quanto l'anonimato impedisce efficacemente la divulgazione non autorizzata, il furto di identità e altre forme di abuso dei dati personali raccolti online, in particolare quando gruppi vulnerabili fanno affidamento su di essi per la loro protezione online;

21. osserva che per alcuni servizi online, per essere pienamente equivalenti ai servizi offline, è necessaria l'identificazione univoca dei loro utenti; rileva che tale identificazione online può essere migliorata applicando l'interoperabilità transfrontaliera delle identificazioni elettroniche prevista dal regolamento eIDAS in tutta l'Unione europea;

22. sottolinea che qualsiasi soluzione di accesso o verifica basata sull'identificazione elettronica deve essere messa a punto nel rispetto del principio di minimizzazione dei dati previsto dal GDPR, in modo che il servizio o la piattaforma che fornisce l'accesso o la verifica basata sull'identificazione elettronica non riceva informazioni sui terzi ai quali accede l'utente e che gli altri dati raccolti siano ridotti al minimo indispensabile; sottolinea che i servizi di accesso o di verifica non dovrebbero essere utilizzati per il tracciamento incrociato degli utenti; ricorda che gli Stati membri e le istituzioni dell'Unione devono garantire che le informazioni elettroniche restino sicure.

[6] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

INFORMAZIONI SULL'APPROVAZIONE
IN SEDE DI COMMISSIONE COMPETENTE PER PARERE

Approvazione	4.2.2021
Esito della votazione finale	+: 60 –: 3 0: 4
Membri titolari presenti al momento della votazione finale	Magdalena Adamowicz, Malik Azmani, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Andrzej Halicki, Balázs Hidvéghi, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Lívia Járóka, Marina Kaljurand, Assita Kanko, Peter Kofod, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Nuno Melo, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Dragoş Tudorache, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Jadwiga Wiśniewska, Elena Yoncheva, Javier Zarzalejos
Supplenti presenti al momento della votazione finale	Anne-Sophie Pelletier, Domènec Ruiz Devesa, Isabel Santos, Tomáš Zdechovský

VOTAZIONE FINALE PER APPELLO NOMINALE
IN SEDE DI COMMISSIONE COMPETENTE PER PARERE

60	+
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Andrzej Halicki, Balázs Hidvéghi, Lívia Járóka, Jeroen Lenaers, Lukas Mandl, Nuno Melo, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Javier Zarzalejos, Tomáš Zdechovský
S&D	Pietro Bartolo, Delara Burkhardt, Caterina Chinnici, Maria Grapini, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Birgit Sippel, Bettina Vollath, Elena Yoncheva
Renew	Malik Azmani, Anna Júlia Donáth, Sophia in ’t Veld, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Dragoş Tudorache
Verts/ALE	Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Terry Reintke, Diana Riba i Giner, Tineke Strik
ID	Nicolaus Fest, Peter Kofod, Annalisa Tardino
ECR	Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Jadwiga Wiśniewska
The Left	Pernando Barrena Arza, Cornelia Ernst, Anne-Sophie Pelletier
NI	Laura Ferrara, Martin Sonneborn

3	-
ID	Marcel de Graaff
The Left	Clare Daly
NI	Milan Uhrík

4	0
S&D	Domènec Ruiz Devesa
ID	Nicolas Bay, Jean-Paul Garraud, Tom Vandendriessche

Significato dei simboli utilizzati:
+ : favorevoli
- : contrari
0 : astenuti