Giovedì 25 marzo 2021

P9_TA(2021)0111

Valutazione della Commissione sull'applicazione del regolamento generale sulla protezione dei dati due anni dopo la sua attuazione

Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP))

(2021/C 494/11)

Il Parlamento europeo,

— visto l'articolo 8 della Carta dei diritti fondamentali,

— visto l'articolo 16 del trattato sul funzionamento dell'Unione europea,

— 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 (regolamento generale sulla protezione dei dati, GDPR) ([1]),

— vista la dichiarazione della Commissione del 24 giugno 2020 sulla sua comunicazione al Parlamento europeo e al Consiglio sulla protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati,

— vista la comunicazione della Commissione al Parlamento europeo e al Consiglio del 24 giugno 2020 sulla protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati (COM(2020)0264),

— vista la comunicazione della Commissione del 24 luglio 2019 dal titolo «Le norme sulla protezione dei dati come strumento generatore di fiducia nell'UE e oltre i suoi confini: un bilancio» (COM(2019)0374),

— visto il contributo del comitato europeo per la protezione dei dati (EDPB) alla valutazione del GDPR a norma dell'articolo 97, adottato il 18 febbraio 2020 ([2]),

— vista la prima panoramica dell'EDPB sull'attuazione del GDPR e sui ruoli e gli strumenti delle autorità nazionali di controllo, del 26 febbraio 2019 ([3]),

— viste le linee guida adottate dall'EDPB a norma dell'articolo 70, paragrafo 1, lettera e), del GDPR,

— visto l'articolo 132, paragrafo 2, del suo regolamento,

— vista la proposta di risoluzione della commissione per le libertà civili, la giustizia e gli affari interni,

A. considerando che il GDPR si applica a decorrere dal 25 maggio 2018; che tutti gli Stati membri ad eccezione della Slovenia hanno adottato una nuova legislazione o adeguato il proprio diritto nazionale in materia di protezione dei dati;

B. considerando che, secondo un'indagine sui diritti fondamentali condotta dall'Agenzia per i diritti fondamentali, le persone sono sempre più consapevoli dei loro diritti a norma del GDPR; che, sebbene le organizzazioni abbiano attuato misure per facilitare l'esercizio dei diritti degli interessati, le persone continuano a incontrare difficoltà quando cercano di esercitare tali diritti, in particolare il diritto di accesso, portabilità e maggiore trasparenza;

C. considerando che, dalla data di inizio dell'applicazione del GDPR, le autorità di controllo hanno registrato un massiccio aumento del numero di reclami ricevuti; che ciò dimostra che gli interessati sono più consapevoli dei propri diritti e vogliono proteggere i propri dati personali in conformità con il GDPR; che tale situazione evidenzia altresì che continuano a essere effettuate numerose operazioni illegali di trattamento dei dati;

([1]) GU L 119 del 4.5.2016, pag. 1.
([2]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf
([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

D. considerando che molte imprese hanno utilizzato il periodo di transizione tra l'entrata in vigore del GDPR e la sua applicazione per una «pulizia» generale dei dati, al fine di valutare quale trattamento dei dati sia effettivamente attuato e quale trattamento potrebbe non essere più necessario o giustificato;

E. considerando che numerose autorità di protezione dei dati non sono in grado di far fronte al numero di reclami ricevuti; che molte di esse presentano carenze di organico e risorse e non dispongono di un sufficiente numero di esperti di tecnologie dell'informazione;

F. considerando che il GDPR riconosce che il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali; che, in base all'articolo 85, la legislazione degli Stati membri dovrebbe prevedere esenzioni al trattamento dei dati effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, qualora esse siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione;

G. considerando che, come altresì sottolineato anche dal comitato europeo per la protezione dei dati, la tutela delle fonti giornalistiche è il caposaldo della libertà di stampa; che il GDPR non dovrebbe essere utilizzato in modo improprio contro i giornalisti e per limitare l'accesso alle informazioni: che esso non dovrebbe in alcun caso essere impiegato dalle autorità nazionali per soffocare la libertà dei media;

Osservazioni generali

1. valuta positivamente il fatto che il GDPR sia diventato il riferimento mondiale in materia di protezione dei dati personali e rappresenti un fattore di convergenza nell'elaborazione delle norme; si compiace del fatto che con l'adozione del GDPR l'UE abbia assunto un ruolo di primo piano nel dibattito internazionale sulla protezione dei dati e che diversi paesi terzi abbiano allineato al GDPR le proprie normative in materia di protezione dei dati; rileva che la Convenzione 108 del Consiglio d'Europa sulla protezione dei dati è stata allineata al GDPR («Convenzione 108+») ed è stata già firmata da 42 paesi; esorta la Commissione e gli Stati membri a sfruttare tale slancio per promuovere a livello delle Nazioni Unite, dell'OCSE, del G8 e del G20 la messa a punto di norme internazionali plasmate sui valori e sui principi europei senza pregiudicare il GDPR; sottolinea che una posizione europea dominante in tale settore aiuterebbe il nostro continente a difendere meglio i diritti dei nostri cittadini, a salvaguardare i nostri valori e principi, a promuovere un'innovazione digitale affidabile e ad accelerare la crescita economica evitando la frammentazione;

2. conclude che, due anni dopo la sua entrata in applicazione, il GDPR può essere globalmente considerato un successo e concorda con la Commissione sul fatto che allo stato attuale non è necessario che sia sottoposto ad aggiornamento o riesame;

3. riconosce che, fino alla prossima valutazione della Commissione, si dovrà continuare a porre l'accento sul miglioramento dell'attuazione e sulle azioni volte a rafforzare l'applicazione del GDPR;

4. prende atto della necessità di un'applicazione rigorosa ed efficace del GDPR presso le piattaforme digitali, le imprese integrate e altri servizi digitali di grandi dimensioni, in particolare nei settori della pubblicità online, del micro-targeting, della profilazione algoritmica, della classificazione, della diffusione e dell'amplificazione dei contenuti;

Base giuridica del trattamento

5. sottolinea che tutte e sei le basi giuridiche stabilite all'articolo 6 del GDPR sono ugualmente valide per il trattamento dei dati personali e che la stessa attività di trattamento può rientrare in più di una base; esorta le autorità di controllo dei dati a precisare che i titolari del trattamento devono fare affidamento su una sola base giuridica per ciascuna finalità delle attività di trattamento, e a specificare in che modo ciascuna base giuridica sia invocata per le loro operazioni di trattamento; esprime preoccupazione per il fatto che i titolari del trattamento spesso citano tutte le basi giuridiche del GDPR nella loro politica in materia di privacy senza un'ulteriore spiegazione e senza fare riferimento alla specifica operazione di trattamento interessata; riconosce che tale approccio ostacola la capacità degli interessati e delle autorità di controllo di valutare se tali basi giuridiche siano appropriate; ricorda che, al fine di trattare categorie particolari di dati personali, occorre individuare una base lecita a norma dell'articolo 6 e una condizione distinta per il trattamento a norma dell'articolo 9; rammenta ai titolari del trattamento il loro obbligo giuridico di effettuare una valutazione d'impatto sulla protezione dei dati qualora sia probabile che il trattamento dei dati comporti un rischio elevato per i diritti e le libertà delle persone fisiche;

6. ricorda che, dall'inizio dell'applicazione del GDPR, per «consenso» si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato; sottolinea che ciò si applica anche alla direttiva e-privacy; rileva che l'attuazione dei requisiti relativi al valido consenso continua a essere compromessa dal ricorso a modelli occulti, a tracciamenti pervasivi e ad altre pratiche non etiche; esprime preoccupazione per il fatto che vengono spesso esercitate pressioni finanziarie per ottenere il consenso degli interessati in cambio di sconti o altre offerte commerciali, come pure per il fatto che l'accesso ai servizi viene spesso subordinato all'ottenimento del consenso sulla base di disposizioni vincolanti, in violazione dell'articolo 7 del GDPR; ricorda che l'EDPB ha armonizzato le norme in merito a cosa costituisce un valido consenso, sostituendo le diverse interpretazioni da parte di molte autorità nazionali di protezione dei dati ed evitando la frammentazione all'interno del mercato unico digitale; ricorda altresì gli orientamenti dell'EDPB e della Commissione che stabiliscono che, nei casi in cui l'interessato abbia inizialmente prestato il suo consenso ma i dati personali siano ulteriormente trattati per una finalità diversa da quella per la quale l'interessato ha prestato il consenso, il consenso iniziale non può legittimare un ulteriore trattamento, in quanto il consenso, per essere valido, deve essere informato e specifico; prende atto degli imminenti orientamenti dell'EDPB sul trattamento dei dati personali per finalità di ricerca scientifica, che forniranno chiarezza sul significato del considerando 50 del GDPR;

7. esprime preoccupazione per il fatto che il «legittimo interesse» è molto spesso citato in modo improprio come base giuridica del trattamento; rileva che i titolari del trattamento continuano a basarsi sul legittimo interesse senza effettuare il necessario esame del bilanciamento degli interessi, che comprende una valutazione dei diritti fondamentali; esprime particolare preoccupazione per il fatto che alcuni Stati membri stanno adottando una legislazione nazionale per determinare le condizioni per il trattamento sulla base del legittimo interesse, prevedendo il bilanciamento dei rispettivi interessi del titolare del trattamento e delle persone interessate, mentre il GDPR obbliga ogni singolo titolare del trattamento a effettuare tale esame del bilanciamento a livello individuale e ad avvalersi di tale fondamento giuridico; teme che alcune interpretazioni nazionali del legittimo interesse non rispettino il considerando 47 e vietino di fatto il trattamento sulla base del legittimo interesse; si compiace che l'EDPB abbia già avviato i lavori per aggiornare il parere del gruppo di lavoro «Articolo 29» sull'applicazione del legittimo interesse quale base giuridica per il trattamento, al fine di affrontare le questioni evidenziate nella relazione della Commissione;

Diritti degli interessati

8. sottolinea che è necessario agevolare l'esercizio dei diritti individuali sanciti dal GDPR, tra cui la portabilità dei dati e i diritti riguardanti il trattamento automatizzato, inclusa la profilazione; accoglie con favore gli orientamenti dell'EDPB sui processi decisionali automatizzati e sulla portabilità dei dati; osserva che in diversi settori il diritto alla portabilità dei dati non è stato pienamente attuato; invita l'EDPB a incoraggiare le piattaforme online a creare un punto di contatto unico per tutte le loro piattaforme digitali sottostanti, da cui le richieste degli utenti possano essere trasmesse al destinatario corretto; rileva che, in linea con il principio della minimizzazione dei dati, l'attuazione del diritto all'anonimato previene efficacemente la divulgazione non autorizzata, il furto d'identità e altre forme di abuso dei dati personali;

9. evidenzia che il rispetto del diritto di essere informato impone alle imprese di fornire informazioni in modo conciso, trasparente, intelligibile e facilmente accessibile e di evitare di adottare un approccio legalistico nell'elaborazione degli avvisi sulla protezione dei dati; esprime preoccupazione per il fatto che talune imprese continuano a violare i loro obblighi di cui all'articolo 12, paragrafo 1, del GDPR e non forniscono tutte le informazioni pertinenti raccomandate dall'EDPB, compreso l'elenco dei nomi dei soggetti con cui condividono i dati; ricorda che l'obbligo di fornire informazioni semplici e accessibili è particolarmente rigoroso per quanto concerne i minori; esprime preoccupazione per l'assenza diffusa di meccanismi di accesso da parte dell'interessato correttamente funzionanti; rileva che le persone spesso non sono in grado di costringere le piattaforme Internet a rivelare i loro profili comportamentali; è preoccupato per il fatto che le imprese ignorano troppo spesso che i dati desunti sono anche dati personali, soggetti a tutte le garanzie previste dal GDPR;

Piccole imprese e organizzazioni

10. osserva che alcune parti interessate segnalano che l'applicazione del GDPR è stata particolarmente complessa, specialmente per le piccole e medie imprese (PMI), le start-up, le organizzazioni e associazioni, ivi comprese le scuole, e i club e le società; osserva, tuttavia, che molti diritti e obblighi previsti dal GDPR non sono nuovi ma erano già prescritti dalla

direttiva 95/46/CE ([4]), sebbene scarsamente applicati; ritiene che il GDPR e la sua applicazione non debbano comportare per le imprese più piccole conseguenze indesiderate a livello di conformità che non verrebbero riscontrate dalle grandi imprese; ritiene che le campagne informative delle autorità nazionali e della Commissione dovrebbero rendere disponibili una maggiore assistenza, informazione e formazione al fine di contribuire a migliorare le conoscenze, la qualità dell'attuazione e la consapevolezza dei requisiti e della finalità del GDPR;

11. sottolinea che non esistono deroghe per le PMI, le start-up, le organizzazioni e associazioni, ivi comprese le scuole, e i club e le società, e che tali entità rientrano all'ambito di applicazione del GDPR; invita pertanto l'EDPB a fornire informazioni chiare per evitare qualsiasi confusione in merito all'interpretazione del GDPR e a creare uno strumento pratico del GDPR per agevolare l'attuazione del regolamento da parte delle PMI, delle start-up, delle organizzazioni e associazioni, ivi comprese le scuole, dei club e delle società che effettuano trattamenti a basso rischio; invita gli Stati membri a mettere a disposizione delle autorità di protezione dei dati sufficienti mezzi affinché possano diffondere le conoscenze circa tali strumenti pratici; incoraggia l'EDPB a sviluppare modelli di politica della privacy ad uso eventuale delle organizzazioni, in modo da aiutarle a dimostrare l'effettiva conformità al GDPR nella pratica, senza dover ricorrere a costosi servizi di terzi;

Attuazione

12. esprime preoccupazione dinanzi all'attuazione disomogenea e talvolta inesistente del GDPR da parte delle autorità nazionali di protezione dei dati a più di due anni dall'inizio dell'applicazione di tale regolamento, e si rammarica pertanto che, in termini di attuazione, la situazione non sia sostanzialmente migliorata rispetto a quella prevista dalla direttiva 95/46/CE;

13. prende atto del fatto che nei primi 18 mesi di applicazione del GDPR sono stati presentati circa 275 000 reclami e sono state imposte 785 sanzioni amministrative per diverse violazioni, ma sottolinea che finora è stato dato seguito solo in minima parte ai reclami presentati; è consapevole dei problemi causati dalle violazioni dei dati personali e ricorda gli attuali orientamenti dell'EDPB che chiariscono, tra l'altro, il calendario per la notifica, la comunicazione agli interessati e i mezzi di ricorso; sottolinea che un modulo standard europeo di notifica delle violazioni dei dati potrebbe essere utile per armonizzare i diversi approcci nazionali; si rammarica, tuttavia, del fatto che l'importo delle sanzioni pecuniarie vari notevolmente da uno Stato membro all'altro e che alcune sanzioni imposte a imprese di grandi dimensioni siano troppo basse per avere l'effetto deterrente previsto per le violazioni della protezione dei dati; invita le autorità di protezione dei dati a rafforzare l'attuazione, il perseguimento e le sanzioni per le violazioni della protezione dei dati e a sfruttare appieno le possibilità previste dal GDPR per l'imposizione di sanzioni pecuniarie, nonché ad avvalersi di altre misure correttive; sottolinea che i divieti di trattamento o l'obbligo di cancellare i dati personali acquisiti in modo non conforme al GDPR possono avere un effetto deterrente pari, se non superiore, alle sanzioni pecuniarie; invita la Commissione e l'EDPB ad armonizzare le sanzioni mediante linee guida e criteri chiari, come è stato fatto dalla conferenza delle autorità di controllo tedesche, al fine di aumentare la certezza giuridica e di evitare che le imprese si stabiliscano nelle zone che impongono le sanzioni più basse;

14. esprime preoccupazione in relazione alla durata delle indagini condotte da alcune autorità di protezione dei dati e alle relative ripercussioni negative sull'efficacia dell'attuazione e la fiducia dei cittadini; sollecita le autorità di protezione dei dati ad accelerare la risoluzione dei casi e ad avvalersi dell'intera gamma di possibilità prevista dal GDPR, in particolare in presenza di violazioni sistematiche e persistenti, anche a scopo di lucro e con un gran numero di interessati;

15. è preoccupato in relazione al fatto che le autorità di controllo di 21 Stati membri dei 31 Stati che applicano il GDPR, vale a dire tutti gli Stati membri dell'Unione europea e dello Spazio economico europeo, e il Regno Unito, hanno dichiarato esplicitamente di non disporre di risorse umane, tecniche e finanziarie, di locali e di infrastrutture sufficienti per adempiere efficacemente i loro compiti ed esercitare i loro poteri; esprime preoccupazione dinanzi alla mancanza di apposito personale tecnico presso la maggior parte delle autorità di controllo in tutta l'UE, cosa che rende difficili le indagini e l'attuazione; constata con preoccupazione che le autorità di controllo sono sotto pressione a causa del crescente squilibrio tra le loro responsabilità nella tutela dei dati personali e le risorse di cui dispongono; osserva che i servizi digitali diventeranno sempre più complessi a causa del maggiore ricorso a innovazioni quali l'intelligenza artificiale (aggravando il problema della limitata trasparenza nel trattamento dei dati, in particolare per la formazione algoritmica); sottolinea

([4]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

pertanto che è importante che le autorità di controllo dell'UE e l'EDPB dispongano di risorse finanziarie, tecniche e umane sufficienti per poter trattare in modo rapido ma approfondito un numero crescente di casi complessi e ad alta intensità di risorse, e per coordinare e agevolare la cooperazione tra le autorità nazionali di protezione dei dati, per monitorare adeguatamente l'applicazione del GDPR e proteggere i diritti e le libertà fondamentali; esprime preoccupazione per il fatto che l'insufficienza delle risorse di cui dispongono le autorità di protezione dei dati — in particolare se si confrontano tali risorse con le entrate delle grandi aziende informatiche — può tradursi in accordi di composizione della controversia, in quanto ciò limiterebbe il costo di procedimenti lunghi e onerosi;

16. invita la Commissione a valutare la possibilità di obbligare le grandi multinazionali tecnologiche a pagare per la propria vigilanza introducendo una tassa dell'UE sul digitale;

17. osserva con preoccupazione che la mancata attuazione da parte delle autorità di protezione dei dati e l'inerzia da parte della Commissione nell'affrontare la carenza di risorse di tali autorità fanno ricadere l'onere dell'attuazione delle norme, e quindi il ricorso a un tribunale per azioni in materia di protezione dei dati, sui singoli cittadini; è preoccupato per il fatto che i tribunali talvolta ordinano il risarcimento dei singoli ricorrenti senza ordinare all'organizzazione o alla società di risolvere i problemi strutturali; considera che l'applicazione delle norme da parte dei privati può determinare un'importante giurisprudenza, ma che non sostituisce l'attuazione da parte delle autorità di protezione dei dati o l'intervento della Commissione per far fronte alla carenza di risorse; si rammarica del fatto che tali Stati membri violino l'articolo 52, paragrafo 4, del GDPR; invita pertanto gli Stati membri a rispettare il loro obbligo giuridico a norma dell'articolo 52, paragrafo 4, di dotare le loro autorità di protezione dei dati di risorse sufficienti per consentire loro di svolgere il proprio lavoro nel miglior modo possibile e assicurare parità di condizioni a livello europeo nell'attuazione del GDPR; si rammarica del fatto che la Commissione non abbia ancora avviato procedure di infrazione nei confronti degli Stati membri che non hanno adempiuto ai loro obblighi nel quadro del GDPR, e sollecita la Commissione a procedere senza indugi in tal senso; invita la Commissione e l'EDPB a organizzare un follow-up della comunicazione della Commissione del 24 giugno 2020, che valuta il funzionamento del GDPR e la sua attuazione;

18. si rammarica del fatto che la maggior parte degli Stati membri abbia deciso di non dare attuazione all'articolo 80, paragrafo 2, del GDPR; invita tutti gli Stati membri ad avvalersi dell'articolo 80, paragrafo 2, e ad attuare il diritto di proporre reclami e di adire i tribunali senza essere incaricati da un interessato; invita gli Stati membri a chiarire, nella legislazione nazionale relativa alle procedure amministrative applicabile alle autorità di controllo, il ruolo dei reclamanti durante le procedure; sottolinea che la legislazione dovrebbe precisare la possibilità di intervento dei reclamanti, che non svolgono un ruolo puramente passivo, nelle diverse fasi della procedura;

Cooperazione e coerenza

19. sottolinea che l'insufficiente livello di attuazione è particolarmente evidente nei reclami transfrontalieri e deplora il fatto che le autorità di protezione dei dati in 14 Stati membri non dispongano di risorse adeguate per contribuire ai meccanismi di cooperazione e coerenza; invita l'EDPB a intensificare gli sforzi volti a garantire la corretta applicazione degli articoli 60 e 63 del GDPR, e ricorda alle autorità di controllo che in circostanze eccezionali possono avvalersi della procedura d'urgenza di cui all'articolo 66 del GDPR, in particolare delle misure provvisorie;

20. sottolinea l'importanza del meccanismo dello sportello unico nell'offrire certezza giuridica e nel ridurre l'onere amministrativo per le imprese e i cittadini; esprime, tuttavia, grande preoccupazione in relazione al funzionamento di tale meccanismo, in particolare per quanto riguarda il ruolo delle autorità di protezione dei dati irlandese e lussemburghese; osserva che dette autorità sono responsabili del trattamento di un gran numero di casi, dal momento che molte aziende tecnologiche hanno registrato la loro sede dell'UE in Irlanda o nel Lussemburgo; è particolarmente preoccupato per via del fatto che l'autorità di protezione dei dati irlandese chiude, in generale, la maggior parte dei casi con una composizione della controversia anziché con una sanzione, e che i casi deferiti all'Irlanda nel 2018 non hanno nemmeno raggiunto la fase di un progetto di decisione a norma dell'articolo 60, paragrafo 3, del GDPR; invita queste autorità di protezione dei dati ad accelerare le indagini in corso su casi importanti, al fine di dimostrare ai cittadini dell'UE che la protezione dei dati è un diritto azionabile nell'Unione; rileva che il successo del meccanismo dello sportello unico dipende dal tempo e dagli sforzi che le autorità di protezione dei dati possono dedicare al trattamento dei singoli casi transfrontalieri e alla cooperazione in merito ad essi in seno all'EDPB, e che la mancanza di volontà politica e di risorse si ripercuote in modo immediato sul corretto funzionamento del meccanismo;

21. osserva alcune incoerenze tra le linee guida degli Stati membri e quelle dell'EDPB; fa notare che le autorità nazionali di protezione dei dati possono giungere a interpretazioni diverse del GDPR, con conseguenti applicazioni divergenti tra gli Stati membri; osserva che tale situazione sta creando vantaggi geografici e svantaggi per le imprese; esorta la Commissione a valutare se le procedure amministrative nazionali ostacolano la piena efficacia della cooperazione a norma dell'articolo 60

del GDPR, così come la sua efficace attuazione; invita le autorità di protezione dei dati ad adoperarsi in vista di un'interpretazione coerente e di orientamenti facilitati dall'EDPB; invita specificamente l'EDPB a stabilire gli elementi essenziali di una procedura amministrativa comune per trattare i reclami nei casi transfrontalieri nell'ambito della cooperazione di cui all'articolo 60; esorta a far sì che ciò avvenga grazie all'elaborazione di orientamenti su tempistiche comuni per lo svolgimento delle indagini e l'adozione delle decisioni; invita l'EDPB a rafforzare il meccanismo di coerenza e a renderlo obbligatorio per qualsiasi questione di applicazione generale o caso che producano effetti transfrontalieri, al fine di evitare, da parte delle singole autorità di protezione dei dati, approcci e decisioni incoerenti, che sarebbero suscettibili di compromettere l'interpretazione e l'applicazione uniformi del GDPR; è del parere che un'interpretazione, un'applicazione e un orientamento comuni contribuiranno alla creazione e al successo del mercato unico digitale;

22. invita l'EDPB a pubblicare prima delle sue riunioni il relativo ordine del giorno e a fornire al pubblico e al Parlamento sintesi più dettagliate delle sue riunioni;

Frammentazione dell'attuazione del GDPR

23. si rammarica del fatto che il ricorso, da parte degli Stati membri, alle clausole di specificazione facoltative (ad esempio, il trattamento nell'interesse pubblico o da parte delle autorità pubbliche sulla base del diritto dello Stato membro e dell'età del consenso dei minori) abbia pregiudicato il conseguimento di una piena armonizzazione della protezione dei dati e l'eliminazione di condizioni di mercato divergenti per le imprese in tutta l'UE, ed esprime preoccupazione in relazione al fatto che ciò può far aumentare il costo della conformità al GDPR; esorta l'EDPB a presentare orientamenti su come affrontare la diversa attuazione delle clausole di specificazione facoltative tra Stati membri; invita la Commissione ad avvalersi dei suoi poteri per intervenire negli Stati membri in cui le misure, le azioni e le decisioni nazionali compromettono lo spirito, l'obiettivo e il testo del GDPR, al fine di evitare una disparità di protezione per i cittadini e distorsioni del mercato; sottolinea in questa fase che gli Stati membri non hanno adottato la stessa fascia di età per il consenso dei genitori; invita pertanto la Commissione e gli Stati membri a valutare l'impatto di questa frammentazione sulle attività dei minori e sulla loro protezione online; sottolinea che, in caso di conflitto di leggi tra una legge nazionale di uno Stato membro e il GDPR, dovrebbero prevalere le disposizioni di quest'ultimo;

24. esprime profonda preoccupazione quanto al ricorso abusivo al GDPR da parte delle autorità pubbliche di alcuni Stati membri al fine di limitare i giornalisti e le organizzazioni non governative; concorda pienamente con la Commissione sul fatto che le norme in materia di protezione dei dati non dovrebbero incidere sull'esercizio della libertà d'espressione e di informazione, in particolare creando un effetto dissuasivo o essendo interpretate come un modo per esercitare pressioni sui giornalisti affinché divulghino le loro fonti; esprime tuttavia la propria delusione dinanzi al fatto che la Commissione non ha ancora concluso la sua valutazione dell'equilibrio tra il diritto alla protezione dei dati personali e la libertà di espressione e di informazione, di cui all'articolo 85 del GDPR; invita la Commissione a terminare senza indebiti ritardi la sua valutazione della legislazione nazionale a tale riguardo e a utilizzare tutti gli strumenti disponibili, comprese le procedure di infrazione, per garantire che gli Stati membri rispettino il GDPR e per limitare la frammentazione del quadro di protezione dei dati;

Protezione dei dati fin dalla progettazione

25. invita le autorità di controllo a valutare l'attuazione dell'articolo 25 relativo alla protezione dei dati fin dalla progettazione e alla protezione per impostazione predefinita, in particolare al fine di garantire le misure tecniche e operative necessarie per l'applicazione dei principi di minimizzazione dei dati e limitazione della finalità, e a determinare l'effetto che tale disposizione ha avuto sui produttori di tecnologie di trattamento; accoglie con favore il fatto che nell'ottobre del 2020 l'EDPB abbia adottato le linee guida 04/2019 sull'articolo 25 relativo alla protezione dei dati fin dalla progettazione e alla protezione per impostazione predefinita, al fine di contribuire alla chiarezza giuridica dei concetti; invita le autorità di controllo a valutare altresì il corretto utilizzo delle impostazioni predefinite di cui all'articolo 25, paragrafo 2, anche da parte di grandi prestatori di servizi online; raccomanda che l'EDPB adotti linee guida per stabilire a quali condizioni specifiche e in quali (classi di) casi i produttori di TIC debbano essere considerati titolari del trattamento ai sensi dell'articolo 4, punto 7, del GDPR, nel senso che determinano i mezzi del trattamento; rileva che le pratiche di protezione dei dati dipendono ancora ampiamente da compiti manuali e formati arbitrari, e sono viziate da sistemi incompatibili; invita l'EDPB a elaborare linee guida che contribuiscano alla messa in pratica dei requisiti in materia di protezione dei dati, ivi comprese linee guida per le valutazioni d'impatto sulla protezione dei dati (articolo 35), la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita (articolo 25), le informazioni da fornire agli interessati (articoli da 12 a 14), l'esercizio dei diritti degli interessati (articoli da 15 a 18, 20 e 21) e i registri delle attività di trattamento (articolo 30); invita l'EDPB a garantire che dette linee guida siano facili da applicare e consentano anche la comunicazione

da macchina a macchina tra gli interessati, i titolari del trattamento e le autorità di protezione dei dati (automatizzazione della protezione dei dati); invita la Commissione a elaborare icone leggibili da dispositivo automatico a norma dell'articolo 12, paragrafo 8, per informare gli interessati, in stretto coordinamento con l'EDPB; incoraggia l'EDPB e le autorità di controllo a sfruttare pienamente il potenziale offerto dall'articolo 21, paragrafo 5, riguardo ai mezzi automatizzati per opporsi al trattamento di dati personali;

Linee guida

26. invita l'EDPB ad armonizzare l'attuazione pratica dei requisiti in materia di protezione dei dati attraverso l'elaborazione di linee guida, in particolare per quanto riguarda la necessità di valutare i rischi associati alle informazioni sul trattamento dei dati fornite agli interessati (articoli da 12 a 14), all'esercizio dei diritti degli interessati (articoli da 15 a 18, 20 e 21) e all'attuazione del principio di responsabilizzazione; invita l'EDPB a formulare linee guida che classifichino diversi casi di usi legittimi della profilazione in base ai loro rischi per i diritti e le libertà degli interessati, unitamente a raccomandazioni concernenti misure tecniche e organizzative appropriate e a una chiara delimitazione dei casi di utilizzo illecito; esorta l'EDPB a rivedere il parere n. 5/2014 del gruppo di lavoro «articolo 29», del 10 aprile 2014, sulle tecniche di anonimizzazione e a istituire un elenco di criteri inequivocabili per il conseguimento dell'anonimizzazione; incoraggia l'EDPB a chiarire il trattamento dei dati per finalità attinenti alle risorse umane; prende atto della conclusione dell'EDPB secondo cui la necessità di valutare i rischi associati al trattamento dei dati, quale prevista dal GDPR, dovrebbe essere mantenuta, dal momento che i rischi per gli interessati non sono legati alla dimensione dei titolari del trattamento; chiede un migliore utilizzo del meccanismo che consente alla Commissione di chiedere consulenze all'EDPB su questioni contemplate dal GDPR;

27. osserva che la pandemia di COVID-19 ha messo in luce la necessità di orientamenti chiari da parte delle autorità di protezione dei dati e dell'EDPB per quanto riguarda l'attuazione e l'applicazione adeguate del GDPR nelle politiche in materia di sanità pubblica; ricorda, a tale riguardo, gli orientamenti n. 3/2020 sul trattamento dei dati relativi alla salute ai fini della ricerca scientifica nel contesto della pandemia di COVID-19 e gli orientamenti n. 4/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto della pandemia di COVID-19; invita la Commissione a garantire il pieno rispetto del GDPR in fase di creazione dello spazio comune europeo di dati sanitari;

Flussi internazionali di dati personali e cooperazione

28. sottolinea l'importanza di consentire la libera circolazione dei dati personali a livello internazionale senza ridurre il livello di protezione garantito dal GPDR; è favorevole all'approccio della Commissione consistente nell'affrontare la protezione dei dati e i flussi di dati personali separatamente dagli accordi commerciali; ritiene che la cooperazione internazionale nel settore della protezione dei dati e la convergenza delle norme pertinenti verso il GDPR miglioreranno la fiducia reciproca, favoriranno la comprensione delle sfide tecnologiche e giuridiche e, in ultima analisi, faciliteranno i flussi di dati transfrontalieri, fondamentali per il commercio internazionale; riconosce che esistono requisiti giuridici contrastanti per le imprese che svolgono attività di trattamento dei dati nell'UE, nonché nelle giurisdizioni di paesi terzi, in particolare negli Stati Uniti;

29. evidenzia che le decisioni di adeguatezza non dovrebbero essere di natura politica, bensì giuridica; incoraggia a proseguire gli sforzi volti a promuovere quadri giuridici globali per consentire i trasferimenti dei dati sulla base del GDPR e della Convenzione 108+ del Consiglio d'Europa; osserva altresì che le parti interessate continuano a considerare le decisioni di adeguatezza uno strumento essenziale per tali flussi di dati, in quanto non introducono condizioni o autorizzazioni vincolanti supplementari; sottolinea, tuttavia, che finora sono state adottate decisioni di adeguatezza solo per nove paesi, anche se molti altri paesi terzi hanno recentemente adottato nuove normative in materia di protezione dei dati con norme e principi simili a quelli del GDPR; rileva che, ad oggi, nessun meccanismo unico che garantisce il trasferimento legale di dati personali commerciali tra l'UE e gli Stati Uniti è stato oggetto di azione giudiziaria dinanzi alla Corte di giustizia dell'Unione europea (CGUE);

30. accoglie con favore l'adozione della prima decisione di adeguatezza reciproca tra l'UE e il Giappone, che ha creato la più vasta area di flussi di dati liberi e sicuri al mondo; invita la Commissione a tenere conto di tutte le questioni sollevate dal Parlamento nella prima revisione di tale strumento e a rendere pubblici quanto prima i risultati, dal momento che la revisione avrebbe dovuto essere adottata entro gennaio del 2021;

31. invita la Commissione a pubblicare i criteri utilizzati per stabilire se un paese terzo offra un livello di protezione «sostanzialmente equivalente» a quello assicurato all'interno dell'Unione, segnatamente per quanto concerne l'accesso ai mezzi di ricorso e l'accesso ai dati da parte del governo; insiste sulla necessità di garantire l'effettiva applicazione e il rispetto

delle disposizioni relative al trasferimento o alla comunicazione non autorizzati dal diritto dell'Unione a norma dell'articolo 48 del GDPR, in particolare per quanto riguarda le richieste di accesso a dati personali nell'Unione da parte delle autorità di paesi terzi, e invita l'EDPB e le autorità di protezione dei dati a fornire orientamenti e ad applicare tali disposizioni, anche in fase di valutazione e sviluppo di meccanismi di trasferimento dei dati personali;

32. invita la Commissione ad adottare atti delegati allo scopo di specificare i requisiti di cui tenere conto ai fini del meccanismo di certificazione della protezione dei dati di cui all'articolo 42, paragrafo 1, in modo da promuovere il ricorso a quest'ultimo, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati, quale strumento per procedere ai trasferimenti internazionali, conformemente all'articolo 46, paragrafo 2, lettera f);

33. ribadisce che i programmi di sorveglianza di massa che prevedono la raccolta di dati in blocco impediscono i riscontri relativi all'adeguatezza; esorta la Commissione ad applicare le conclusioni della CGUE nelle cause Schrems I ([5]), II ([6]) e Privacy International & a. (2020) ([7]) a tutte le revisioni delle decisioni di adeguatezza, nonché ai negoziati in corso e futuri; ricorda che i trasferimenti che si basano su deroghe in specifiche situazioni a norma dell'articolo 49 del GDPR dovrebbero rimanere eccezionali; accoglie con favore le linee guide dell'EDPB e delle autorità di protezione dei dati al riguardo e invita tali organismi a garantire un'interpretazione coerente nell'applicazione e nel controllo di tali deroghe, in linea con le linee guida n. 2/2018 dell'EDPB;

34. invita le autorità di protezione dei dati e la Commissione a valutare in modo sistematico se le norme in materia di protezione dei dati siano applicate nella pratica nei paesi terzi, in linea con la giurisprudenza della CGUE;

35. esorta la Commissione a pubblicare senza indebito ritardo il riesame delle decisioni di adeguatezza adottate a norma della direttiva del 1995; sottolinea che, in assenza di una decisione di adeguatezza, le clausole contrattuali tipo sono lo strumento più utilizzato per i trasferimenti internazionali di dati; osserva che la CGUE ha sostenuto la validità della decisione 2010/87/UE relativa alle clausole contrattuali tipo ([8]), esigendo nel contempo una valutazione del livello di protezione concesso ai dati trasferiti a un paese terzo e degli aspetti pertinenti dell'ordinamento giuridico di detto paese terzo per quanto riguarda l'accesso delle autorità pubbliche ai dati personali trasferiti; esorta la Commissione ad accelerare il suo lavoro sulla modernizzazione delle clausole contrattuali tipo per i trasferimenti internazionali di dati, al fine di garantire condizioni di parità per le piccole e medie imprese (PMI) a livello internazionale; accoglie positivamente la pubblicazione da parte della Commissione di un progetto di clausole contrattuali tipo e l'obiettivo di rendere queste ultime più facili da utilizzare e di affrontare le carenze individuate delle norme vigenti;

36. rammenta le linee guida n. 1/2019 dell'EDPB sui codici di condotta e gli organismi di monitoraggio di cui al regolamento (UE) 2016/679; riconosce che, al momento, tale strumento non è sufficientemente utilizzato nonostante garantisca la conformità al GDPR se associato a un impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate; evidenzia che tale strumento è potenzialmente in grado di offrire un migliore sostegno alle PMI e di fornire maggiore certezza giuridica nel contesto dei trasferimenti internazionali di dati tra diversi settori;

Legislazione dell'Unione futura

37. ritiene che il GDPR, essendo tecnologicamente neutro, rappresenti un valido quadro normativo per le tecnologie emergenti; è tuttavia del parere che siano necessari ulteriori sforzi per affrontare le questioni più ampie della digitalizzazione, quali le situazioni di monopolio e gli squilibri di potere attraverso una regolamentazione specifica, e per valutare attentamente la correlazione tra il GDPR e ogni nuova iniziativa legislativa, in modo da garantire la coerenza

([5]) Sentenza della Corte di giustizia del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

([6]) Sentenza della Corte di giustizia del 16 luglio 2020, *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

([7]) Sentenze nella causa C-623/17, *Privacy International*, e nelle cause riunite C-511/18, *La Quadrature du Net e a.*, C-512/18, *French Data Network e a.*, e C-520/18, *Ordre des barreaux francophones e germanophone e a.*.

([8]) Decisione 2010/87/UE della Commissione del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, quale modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione del 16 dicembre 2016 (GU L 39 del 12.2.2010, pag. 5).

e colmare le lacune giuridiche; ricorda alla Commissione il suo obbligo di garantire che le proposte legislative, ad esempio quelle relative alla governance dei dati, alla legge sui dati, alla legge sui servizi digitali o sull'intelligenza artificiale, siano sempre pienamente conformi al GDPR e alla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie ([9]); ritiene che i testi definitivi adottati dai colegislatori al termine di negoziati interistituzionali debbano rispettare appieno l'acquis in materia di protezione dei dati; si rammarica tuttavia che la Commissione stessa non adotti sempre un approccio coerente alla protezione dei dati nelle proposte legislative; sottolinea che un riferimento all'applicazione del GDPR o l'espressione «fatto salvo il GDPR» non garantiscono automaticamente la conformità della proposta al regolamento; invita la Commissione a consultare il Garante europeo della protezione dei dati e l'EDPB ogniqualvolta l'adozione di una proposta di atto legislativo influisca sulla protezione dei diritti e delle libertà delle persone per quanto riguarda il trattamento di dati personali; invita la Commissione a impegnarsi a consultare il Garante europeo della protezione dei dati durante l'elaborazione di proposte o raccomandazioni, in modo da garantire la coerenza delle norme in materia di protezione dei dati in tutta l'Unione, e a realizzare sempre una valutazione d'impatto;

38. rileva che, nonostante sia permessa dall'articolo 22 del GDPR solo a condizioni rigorose e restrittive, la profilazione è impiegata sempre più spesso, dal momento che le attività online delle persone consentono di avere una conoscenza approfondita della loro psicologia e della loro vita privata; rileva che, poiché la profilazione permette di manipolare il comportamento degli utenti, la raccolta e il trattamento di dati personali relativi all'utilizzo dei servizi digitali dovrebbero essere limitati a quanto strettamente necessario per fornire il servizio e addebitarne il costo agli utenti; invita la Commissione a proporre una rigorosa normativa settoriale in materia di protezione dei dati per le categorie sensibili di dati personali, laddove non l'abbia ancora fatto; chiede la rigorosa applicazione del GDPR nel trattamento di dati personali;

39. chiede che i consumatori siano messi nelle condizioni di prendere decisioni informate sulle conseguenze per la vita privata derivanti dall'utilizzo delle nuove tecnologie e che sia garantito un trattamento equo e trasparente, mettendo a loro disposizione opzioni di facile utilizzo per accordare e revocare il proprio consenso al trattamento dei dati personali, conformemente a quanto stabilito dal GDPR;

Direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie

40. è preoccupato che le norme in materia di protezione dei dati utilizzate a fini di contrasto siano ampiamente inadeguate a tenere il passo con le nuove competenze in tale ambito; invita pertanto la Commissione a valutare la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie entro il termine previsto dalla direttiva e a rendere la revisione pubblicamente disponibile;

Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche

41. esprime profonda preoccupazione per la mancata attuazione da parte degli Stati membri della direttiva relativa alla vita privata e alle comunicazioni elettroniche ([10]) alla luce delle modifiche introdotte dal GDPR; invita la Commissione ad accelerare la propria valutazione e ad avviare procedure di infrazione nei confronti degli Stati membri che non hanno attuato correttamente la direttiva; è fortemente preoccupato che la riforma della direttiva relativa alla vita privata e alle comunicazioni elettroniche, necessaria già diversi anni fa, comporti una frammentazione del panorama giuridico nell'UE, a scapito sia delle imprese che dei cittadini; ricorda che il regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche ([11]) è stato concepito in modo da integrare e precisare il GDPR e da coincidere con l'entrata in applicazione di quest'ultimo; sottolinea che la riforma della regolamentazione in materia di vita privata e comunicazioni elettroniche non deve ridurre il livello di protezione garantito dal GDPR e dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche; si rammarica per il fatto che il Consiglio abbia impiegato quattro anni per adottare la propria posizione negoziale sulla proposta di regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche, mentre il Parlamento ha adottato la propria posizione negoziale nell'ottobre 2017; ricorda l'importanza di aggiornare la regolamentazione in materia di vita privata e comunicazioni elettroniche del 2002 e del 2009 al fine di migliorare la tutela dei diritti fondamentali dei cittadini e la certezza giuridica per le imprese, a integrazione del GDPR;

([9]) 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).

([10]) 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 (GU L 201 del 31.7.2002, pag. 37).

([11]) Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (COM(2017)0010).

o

o o

42. incarica il suo Presidente di trasmettere la presente risoluzione alla Commissione, al Consiglio europeo, ai governi e ai parlamenti nazionali, al comitato europeo per la protezione dei dati e al Garante europeo della protezione dei dati.