Parlamento europeo
2014-2019

TESTI APPROVATI

P8_TA(2017)0076

Implicazioni dei Big Data in termini di diritti fondamentali

Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI))

Il Parlamento europeo,

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

– visti gli articoli 1, 7, 8, 11, 14, 21, 47 e 52 della Carta dei diritti fondamentali dell'Unione europea,

– visti gli orientamenti per la gestione degli schedari computerizzati di dati personali contenuti nella risoluzione 45/95 del 14 dicembre 1990 dell'Assemblea generale delle Nazioni Unite,

– visti 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)[1] e 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[2],

– vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, del 6 maggio 2015, intitolata "Strategia per il mercato unico digitale in Europa" (COM(2015)0192),

– visti la convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE n. 108), del 28 gennaio 1981, e il suo protocollo aggiuntivo dell'8 novembre 2001 (STE n. 181)[3],

---

1 GU L 119 del 4.5.2016, pag. 1.
2 GU L 119 del 4.5.2016, pag. 89.
3 http://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/108

– vista la raccomandazione CM/Rec(2010)13 del Comitato dei Ministri del Consiglio d'Europa agli Stati membri sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nel contesto delle attività di profilazione, del 23 novembre 2010[1],

– visto il parere 7/2015 del Garante europeo della protezione dei dati, del 19 novembre 2015, dal titolo "Meeting the challenges of big data – A call for transparency, user control, data protection by design and accountability" ("Affrontare le sfide dei Big Data: un invito alla trasparenza, al controllo dell'utente, alla protezione dei dati fin dalla progettazione e alla responsabilità")[2],

– visto il parere 8/2016 del Garante europeo della protezione dei dati, del 23 settembre 2016, dal titolo "EDPS Opinion on coherent enforcement of fundamental rights in the age of big data" (Parere del Garante europeo della protezione dei dati sull'applicazione coerente dei diritti fondamentali nell'era dei Big Data)[3],

– vista la dichiarazione del 16 settembre 2014 del gruppo di lavoro sulla protezione dei dati "Articolo 29" relativa all'impatto dello sviluppo dei Big Data sulla protezione delle persone rispetto al trattamento automatizzato dei loro dati personali nell'UE[4],

– visto l'articolo 52 del suo regolamento,

– vista la relazione della commissione per le libertà civili, la giustizia e gli affari interni (A8-0044/2017),

A. considerando che i Big Data si riferiscono alla raccolta, all'analisi e all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli (analisi dei Big Data);

B. considerando che determinati casi di uso dei Big Data riguardano l'addestramento degli strumenti di intelligenza artificiale come le reti neuronali e i modelli statistici al fine di prevedere determinati eventi e comportamenti; che i dati usati per l'addestramento sono spesso di qualità discutibile e non neutrale;

C. considerando che i progressi delle tecnologie di comunicazione e l'uso massiccio di dispositivi elettronici e di monitoraggio, dei social media, delle interazioni e delle reti web, compresi i dispositivi che comunicano informazioni senza intervento umano, hanno portato allo sviluppo di enormi insiemi di dati in costante crescita che, attraverso l'analisi e tecniche avanzate di trattamento, tracciano un quadro senza precedenti del comportamento umano, della vita privata e delle nostre società;

---

1 https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00

2 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

3 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-09-23_BigData_opinion_EN.pdf

4 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

D. considerando che i servizi di intelligence dei paesi terzi e degli Stati membri ricorrono con sempre maggiore frequenza al trattamento e all'analisi di tali insiemi di dati che non sono disciplinati da alcun quadro giuridico o, come avvenuto di recente, sono oggetto di una normativa la cui compatibilità con il diritto primario e secondario dell'Unione è fonte di preoccupazione e deve ancora essere accertata;

E. considerando che l'aumento del bullismo, della violenza contro le donne e della vulnerabilità dei minori si verifica anche su Internet; che la Commissione e gli Stati membri dovrebbero adottare tutte le misure giuridiche necessarie per contrastare questi fenomeni;

F. considerando che un numero crescente di società, imprese, enti e agenzie, organizzazioni governative e non governative (come pure il settore pubblico e quello privato in generale), leader politici nonché società civile, mondo accademico, comunità scientifica e cittadini nel complesso hanno sfruttato tali insiemi di dati e l'analisi dei Big Data per promuovere la competitività, l'innovazione, le previsioni di mercato, le campagne politiche, la pubblicità mirata, la ricerca scientifica e la definizione delle politiche nel settore dei trasporti, del fisco, dei servizi finanziari, delle città intelligenti, dell'applicazione della legge, della trasparenza, della salute pubblica e della risposta alle catastrofi, come pure per influenzare le elezioni e i risultati politici tramite, ad esempio, la comunicazione mirata;

G. considerando che il mercato dei Big Data è in crescita grazie al fatto che la tecnologia e il processo decisionale basato sui dati sono considerati fonti di soluzioni sempre più accettate; che non esiste ancora una metodologia che consenta di effettuare una valutazione basata su riscontri oggettivi dell'impatto complessivo dei Big Data, ma esistono elementi indicanti che l'analisi dei Big Data può avere un impatto orizzontale significativo sia sul settore pubblico che su quello privato; che la strategia per il mercato unico digitale in Europa della Commissione riconosce il potenziale delle tecnologie e dei servizi basati sui dati nonché dei Big Data quali catalizzatori di crescita economica, innovazione e digitalizzazione nell'UE;

H. considerando che l'analisi dei Big Data crea valore aggiunto in vari modi, dimostrati da numerosi esempi, che generano opportunità significative per i cittadini, ad esempio nell'ambito dell'assistenza sanitaria, della lotta ai cambiamenti climatici, della riduzione del consumo energetico, del miglioramento della sicurezza dei trasporti e del funzionamento delle città intelligenti, potenziando in tal modo l'ottimizzazione e l'efficienza delle imprese e contribuendo a migliorare le condizioni di lavoro nonché a individuare e combattere le frodi; che i Big Data possono fornire un vantaggio competitivo ai processi decisionali delle imprese europee, mentre il settore pubblico può trarre vantaggio da una maggiore efficienza grazie a una conoscenza più ampia dei diversi livelli di sviluppo socio-economico;

I. considerando che i Big Data possono apportare i summenzionati benefici a cittadini, mondo accademico, comunità scientifica e settore pubblico e privato, ma comportano anche rischi significativi, in particolare per quanto riguarda la protezione dei diritti fondamentali, quali il diritto alla privacy, alla protezione dei dati e alla loro sicurezza, come pure la libertà di espressione e di non discriminazione, che sono garantiti dalla Carta dei diritti fondamentali e dal diritto dell'Unione; che le tecniche di pseudonimizzazione e di crittografia possono mitigare i rischi legati all'analisi dei Big Data e svolgere quindi un ruolo importante nel salvaguardare la privacy dell'interessato,

promuovendo nel contempo l'innovazione e la crescita economica; che tali elementi devono essere considerati nell'ambito dell'attuale revisione della direttiva e-privacy;

J. considerando che il grado di diffusione dei sensori, l'ampia produzione sistematica di dati e le odierne attività di trattamento dei dati non presentano sempre l'adeguata trasparenza e mettono alla prova la capacità dei singoli e delle autorità di valutare i processi e le finalità della raccolta, della compilazione, dell'analisi e dell'utilizzo dei dati personali; che dall'impiego dell'analisi dei Big Data si osserva una confusione tra i dati personali e quelli non personali, il che può portare alla creazione di nuovi dati personali;

K. considerando che il settore dei Big Data cresce del 40 % all'anno, sette volte più velocemente del mercato delle tecnologie dell'informazione; che la concentrazione di grandi insiemi di dati prodotti dalle nuove tecnologie offre informazioni essenziali per le grandi aziende, il che innesca cambiamenti senza precedenti nei rapporti di forza tra cittadini, governi e attori privati; che tale concentrazione di poteri nelle mani delle imprese potrebbe consolidare i monopoli e le pratiche abusive nonché avere un effetto dannoso sui diritti dei consumatori e su un'equa concorrenza di mercato; che l'interesse dei singoli e la protezione dei diritti fondamentali dovrebbero essere ulteriormente analizzati nell'ambito delle fusioni di Big Data;

L. considerando che i Big Data presentano un enorme potenziale inespresso in qualità di motori della produttività e strumenti in grado di offrire ai cittadini prodotti e servizi migliori; che è opportuno tuttavia sottolineare che l'uso generalizzato di dispositivi intelligenti, reti e applicazioni digitali da parte di cittadini, imprese e organizzazioni non è necessariamente indice di soddisfazione rispetto ai prodotti offerti, quanto piuttosto di una consapevolezza generale del fatto che tali servizi sono diventati indispensabili per vivere, comunicare e lavorare, nonostante la mancata comprensione dei rischi che essi potrebbero comportare per il benessere, la sicurezza e i diritti delle persone;

M. considerando che è opportuno operare una distinzione fra quantità e qualità dei dati, onde agevolare l'uso efficace dei Big Data (algoritmi e altri strumenti analitici); che dati e/o procedure di scarsa qualità alla base dei processi decisionali e degli strumenti analitici potrebbero portare ad algoritmi imparziali, correlazioni spurie, errori, sottostima delle implicazioni giuridiche, sociali ed etiche, rischio che i dati siano impiegati per finalità discriminatorie e fraudolente nonché marginalizzazione del ruolo degli esseri umani in tali processi, il che avrebbe come conseguenza procedure decisionali viziate che possono avere un impatto deleterio sulla vita e sulle opportunità dei cittadini, in particolare dei gruppi emarginati, nonché influenzare negativamente le società e le imprese;

N. considerando che la responsabilità e la trasparenza a livello degli algoritmi dovrebbero riflettere l'applicazione di misure tecniche e operative che assicurino la trasparenza, la non discriminazione del processo decisionale automatizzato e il calcolo delle probabilità del singolo comportamento; che la trasparenza dovrebbe offrire alle persone informazioni significative sulla logica utilizzata, l'importanza e le conseguenze previste; che ciò dovrebbe includere informazioni sui dati utilizzati per formare l'analisi dei Big Data e permettere alle persone di comprendere e monitorare le decisioni che le riguardano;

O. considerando che l'analisi dei dati e gli algoritmi influenzano sempre di più le informazioni rese accessibili ai cittadini; che tali tecniche, se utilizzate impropriamente,

possono mettere in pericolo i diritti fondamentali all'informazione, nonché la libertà dei mezzi di comunicazione e il pluralismo; che il sistema di radiodiffusione pubblica negli Stati membri è direttamente collegato alle esigenze democratiche, sociali e culturali di ogni società, nonché alla necessità di preservare il pluralismo dei mezzi di comunicazione, come indicato nel protocollo sul sistema di radiodiffusione pubblica negli Stati membri allegato al trattato di Amsterdam (11997D/PRO/09);

P. considerando che la proliferazione del trattamento e dell'analisi dei dati, l'elevato numero di soggetti coinvolti nella raccolta, nella conservazione, nel trattamento e nella condivisione dei dati e la combinazione di grandi insiemi di dati contenenti dati personali e non personali provenienti da una serie di fonti diverse, seppur generando opportunità significative, hanno creato una grande incertezza sia per i cittadini che per il settore pubblico e per quello privato relativamente ai requisiti specifici per la conformità alla vigente legislazione dell'UE in materia di protezione dei dati;

Q. considerando che esiste una moltitudine di sistemi preesistenti non strutturati che contengono grandi volumi di dati raccolti dalle imprese nel corso di molti anni con sistemi di gestione dei dati poco chiari, i quali vanno resi sistematicamente conformi;

R. considerando che è opportuno favorire una maggiore cooperazione e coerenza tra le varie autorità di regolamentazione e di vigilanza della concorrenza, di tutela dei consumatori e di protezione dei dati a livello nazionale e dell'UE, al fine di garantire un approccio coerente alle implicazioni dei Big Data per i diritti fondamentali e la loro comprensione; che l'istituzione e l'ulteriore sviluppo di una struttura di coordinamento digitale[1] (Digital Clearing House), in qualità di rete volontaria di organismi di contrasto, può contribuire a migliorarne le operazioni e le rispettive attività di contrasto nonché aiutare a rafforzare le sinergie e la tutela dei diritti e degli interessi degli individui;

Considerazioni generali

1. evidenzia che i cittadini, il settore pubblico e quello privato, il mondo accademico e la comunità scientifica possono godere appieno delle prospettive e delle opportunità offerte dai Big Data, solo se la fiducia pubblica in tali tecnologie è garantita da una rigorosa applicazione dei diritti fondamentali, dalla conformità alla vigente legislazione dell'UE in materia di protezione dei dati nonché dalla certezza giuridica per tutti i soggetti coinvolti; sottolinea che il trattamento dei dati personali può essere effettuato solo a norma delle basi giuridiche stabilite all'articolo 6 del regolamento (UE) 2016/679; ritiene fondamentale che la trasparenza e l'adeguata offerta di informazioni al pubblico interessato costituiscano elementi essenziali della costruzione della fiducia pubblica e della protezione dei diritti individuali;

2. sottolinea che la conformità con la vigente legislazione in materia di protezione dei dati, unitamente a solide norme scientifiche ed etiche sono fondamentali per creare fiducia nelle soluzioni dei Big Data e considerarle affidabili; evidenzia inoltre che le informazioni emerse grazie all'analisi dei Big Data non offrono quadri imparziali di alcun tema e sono affidabili solo nella misura consentita dai dati di riferimento; pone l'accento sul fatto che l'analisi predittiva basata sui Big Data è in grado di offrire solo una probabilità statistica e, pertanto, non può mai anticipare con precisione il

---

[1] Parere 8/2016 del Garante europeo della protezione dei dati, del 23 settembre 2016, pag. 15.

comportamento individuale; sottolinea pertanto che solide norme scientifiche ed etiche sono essenziali per gestire la raccolta dei dati e valutare i risultati di tale analisi;

3. sottolinea che le informazioni sensibili sulle persone possono essere dedotte da dati non sensibili, circostanza che rende poco chiara la distinzione tra dati sensibili e non sensibili;

4. sottolinea che la scarsa conoscenza e comprensione da parte dei singoli della natura dei Big Data consente l'utilizzo di informazioni personali in modi non intenzionali; rileva che la formazione e la sensibilizzazione sui diritti fondamentali sono estremamente urgenti nell'Unione; esorta le istituzioni dell'UE e gli Stati membri a investire nell'alfabetizzazione digitale e nella sensibilizzazione in merito ai diritti digitali, alla privacy e alla protezione dei dati tra i cittadini, compresi i minori; sottolinea che questo tipo di formazione dovrebbe contemplare la conoscenza dei principi o delle logiche di funzionamento degli algoritmi e dei processi decisionali automatizzati nonché del modo per interpretarli in maniera significativa; evidenzia inoltre la necessità di formare promuovendo la conoscenza dei luoghi e delle modalità di raccolta dei flussi di dati (ossia web scraping, combinazione dei dati di streaming con i dati delle reti sociali e dei dispositivi collegati e aggregazione degli stessi in un nuovo flusso di dati);

I Big Data a fini commerciali e nel settore pubblico

Privacy e protezione dei dati

5. sottolinea che la legislazione dell'Unione in materia di protezione della privacy e dei dati personali, il diritto all'uguaglianza e alla non discriminazione nonché il diritto dei singoli di ricevere informazioni riguardanti le logiche sottostanti ai processi decisionali automatizzati e alla profilazione, come pure il diritto di ricorso sono applicabili al trattamento dei dati anche quando questo è preceduto da tecniche di pseudonimizzazione e, in ogni caso, quando l'uso dei dati non personali può ripercuotersi sulla sfera privata dei singoli o su altri diritti e libertà, con la conseguente stigmatizzazione di interi gruppi di popolazione;

6. sottolinea che il mercato unico digitale deve fondarsi su reti e servizi affidabili, sicuri e ad alta velocità che tutelino i diritti fondamentali dell'interessato alla protezione dei dati e alla privacy, incoraggiando nel contempo l'innovazione e l'analisi dei Big Data al fine di creare le giuste condizioni e garantire parità di trattamento per rilanciare l'economia europea digitale;

7. mette in evidenza anche la possibilità di reidentificare i singoli correlando le diverse tipologie di dati anonimi; sottolinea che la legislazione dell'Unione in materia di protezione della privacy e dei dati personali si applica al trattamento di tali dati correlati solo quando una persona è effettivamente reidentificabile;

8. mette in risalto che i suddetti principi dovrebbero fungere da quadro di riferimento per il processo decisionale nei settori pubblico e privato e per altri soggetti che utilizzano i dati; pone enfasi sulla necessità di una responsabilità e una trasparenza ancora maggiori a livello di algoritmo per quanto concerne il trattamento e l'analisi dei dati da parte del settore pubblico, di quello privato e di qualsiasi altro attore che ricorre all'analisi dei dati, quale strumento essenziale per garantire che l'interessato sia debitamente informato del trattamento dei propri dati personali;

9. evidenzia il ruolo fondamentale che la Commissione, il Comitato europeo per la protezione dei dati, le autorità nazionali di protezione dei dati e le altre autorità di controllo indipendenti dovrebbero svolgere in futuro per promuovere la trasparenza e il giusto processo, la certezza giuridica in generale e, nello specifico, misure concrete volte a tutelare i diritti fondamentali e le garanzie associate al ricorso al trattamento e all'analisi dei dati da parte del settore pubblico e di quello privato; chiede una più stretta cooperazione tra le autorità di regolamentazione dei comportamenti nell'ambiente digitale, al fine di potenziare le sinergie tra i quadri normativi per i consumatori e per le autorità per la concorrenza e la protezione dei dati; chiede inoltre di dotare tali autorità di fondi e personale in misura adeguata; riconosce altresì la necessità di istituire una struttura di coordinamento digitale;

10. sottolinea che l'obiettivo intrinseco dei Big Data dovrebbe essere quello di ottenere correlazioni comparabili impiegando il numero minimo possibile di dati personali; sottolinea, a tale proposito, che la scienza, le imprese e le comunità pubbliche dovrebbero concentrarsi sulla ricerca e l'innovazione nel settore dell'anonimizzazione;

11. riconosce che applicando la pseudonimizzazione, l'anonimizzazione o la crittografia ai dati personali è possibile ridurre i rischi per gli interessati quando i dati personali sono utilizzati in applicazioni di Big Data; sottolinea inoltre i vantaggi della pseudonimizzazione prevista dal regolamento generale sulla protezione dei dati, quale misura di sicurezza adeguata; ricorda che l'anonimizzazione è un processo irreversibile in virtù del quale i dati personali non possono più essere utilizzati da soli per identificare o isolare una persona fisica; è del parere che gli obblighi contrattuali dovrebbero garantire che i dati anonimi siano reidentificati per mezzo di correlazioni aggiuntive che mettano insieme fonti di dati diverse; invita il settore pubblico e quello privato, come pure gli altri attori coinvolti nell'analisi dei Big Data a riesaminare periodicamente tali rischi alla luce delle nuove tecnologie e a documentare l'adeguatezza delle misure adottate; chiede alla Commissione, al Comitato europeo per la protezione dei dati e alle altre autorità di controllo indipendenti di elaborare orientamenti sulle modalità per rendere anonimi tali dati in modo adeguato, onde evitare abusi futuri di tali misure e monitorare le prassi;

12. esorta il settore pubblico, quello privato e gli altri titolari del trattamento dei dati ad avvalersi degli strumenti previsti dal regolamento generale sulla protezione dei dati, come ad esempio i codici di condotta e i sistemi di certificazione, per garantire una maggiore certezza quanto ai loro obblighi specifici a norma del diritto dell'Unione e rendere le loro pratiche e attività conformi alle opportune norme giuridiche e garanzie dell'UE;

13. chiede alle Commissione e agli Stati membri di garantire che le tecnologie basate sui dati non restringano o discriminino l'accesso a un ambiente mediatico pluralistico, ma, al contrario, favoriscano la libertà e il pluralismo dei media; evidenzia che la cooperazione tra i governi, gli istituti di istruzione e le organizzazioni dei media svolgerà un ruolo fondamentale nel garantire il sostegno all'alfabetizzazione mediatica digitale al fine di responsabilizzare i cittadini e proteggerne i diritti all'informazione e alla libertà di espressione;

14. è del parere che la pubblicazione di dati personali da parte di autorità pubbliche per motivi di interesse pubblico, quali la prevenzione della corruzione, dei conflitti di interesse, delle frodi fiscali e del riciclaggio di denaro, può essere ammissibile in una

società democratica, a condizione che i dati vengano divulgati alle condizioni stabilite dalla legge, che siano in atto misure di sicurezza adeguate e che tale pubblicazione sia necessaria e proporzionata allo scopo perseguito;

Sicurezza

15. riconosce il valore aggiunto dello sviluppo tecnologico che contribuirà a migliorare la sicurezza; prende atto del fatto che alcuni dei rischi più urgenti legati alle attività di trattamento dei dati, come le tecniche relative ai Big Data (in particolare nell'ambito dell'"Internet delle cose"), e che destano preoccupazione tra le persone comprendono le violazioni della sicurezza, l'accesso non autorizzato ai dati e la sorveglianza illegale; ritiene che per contrastare tali minacce senza violare i diritti fondamentali sia necessaria una vera cooperazione concertata tra il settore privato, il settore pubblico, le autorità di contrasto e le autorità di controllo indipendenti; sottolinea, in proposito, che è opportuno prestare un'attenzione particolare alla sicurezza dei sistemi di e-government e a misure giuridiche aggiuntive, come la responsabilità dei software;

16. è del parere che dovrebbe essere incoraggiato e, ove necessario, reso obbligatorio anche il ricorso alla crittografia da punto a punto, secondo il principio della protezione dei dati fin dalla progettazione; raccomanda di far sì che qualsiasi quadro legislativo futuro in tal senso proibisca specificamente ai fornitori di servizi di crittografia, ai fornitori di servizi di comunicazione e a tutte le altre organizzazioni (a tutti i livelli della catena di approvvigionamento) di consentire o agevolare le "backdoor";

17. evidenzia che l'accresciuta generazione e i maggiori flussi di dati comportano ulteriori vulnerabilità e nuove sfide a livello della sicurezza delle informazioni; chiede, a tale proposito, di utilizzare la privacy fin dalla progettazione e per impostazione predefinita, le tecniche di anonimizzazione e, ove del caso, di crittografia nonché di condurre valutazioni obbligatorie dell'impatto sulla privacy; sottolinea che tali misure dovrebbero essere applicate da tutti gli attori coinvolti nell'analisi dei Big Data nei settori pubblico e privato, come pure da altri attori che si occupano di dati sensibili, come ad esempio avvocati, giornalisti e persone che lavorano nel settore sanitario, in modo da garantire che i Big Data non aumentino l'esposizione delle informazioni ai rischi della sicurezza;

18. ricorda che, conformemente all'articolo 15 della direttiva 2000/31/CE, gli Stati membri non impongono ai prestatori dei servizi di trasmissione, memorizzazione e hosting un obbligo generale di vigilanza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite; rammenta, in particolare, che la Corte di giustizia dell'Unione europea, nelle cause C-360/10 e C-70/10, ha respinto le misure di "sorveglianza attiva" della quasi totalità degli utenti dei servizi interessati (fornitori di accesso a Internet in un caso, rete sociale nell'altro) e ha precisato che è vietata qualsiasi ingiunzione che imponga al prestatore di servizi di hosting una sorveglianza generale;

Non discriminazione

19. sottolinea che, a causa degli insiemi di dati e dei sistemi algoritmici utilizzati per le valutazioni e le previsioni nelle varie fasi del trattamento dei dati, i Big Data possono condurre non solo a violazioni dei diritti fondamentali dei singoli, ma anche a una disparità di trattamento e a una discriminazione indiretta nei confronti di gruppi di persone con caratteristiche simili, in particolare per quanto concerne l'equità e le pari

opportunità di accesso all'istruzione e all'occupazione, quando si offre un lavoro alla persona o la si valuta oppure quando si determinano le nuove abitudini di consumo degli utenti dei media sociali;

20. invita la Commissione, gli Stati membri e le autorità di protezione dei dati a individuare e adottare tutte le misure opportune per ridurre al minimo la discriminazione e la mancanza di imparzialità algoritmiche, nonché a sviluppare un solido quadro etico comune per la trasparenza nel trattamento dei dati personali e nel processo decisionale automatizzato, che possa orientare l'utilizzo dei dati e guidare la costante applicazione del diritto dell'Unione;

21. invita la Commissione, gli Stati membri e le autorità di protezione dei dati a valutare specificamente la necessità non solo della trasparenza algoritmica, ma anche della trasparenza sulle possibili distorsioni nei dati di formazione utilizzati per formulare deduzioni sulla base dei Big Data;

22. raccomanda che le imprese conducano valutazioni periodiche del livello di rappresentatività degli insiemi di dati, valutino se essi presentano elementi non imparziali e sviluppino strategie per superare tali problemi; evidenzia la necessità di riesaminare l'accuratezza e la significatività delle previsioni basate sulle analisi dei dati alla luce dell'equità e delle preoccupazioni di ordine etico;

I Big Data a fini scientifici

23. sottolinea che le analisi dei Big Data possono essere utili per il progresso scientifico e la ricerca; ritiene che lo sviluppo e l'impiego delle analisi dei Big Data a fini scientifici dovrebbero avvenire nel debito rispetto dei valori fondamentali sanciti nella Carta dei diritti fondamentali e in conformità della vigente legislazione dell'UE in materia di protezione dei dati;

24. ricorda che, ai sensi del regolamento generale sulla protezione dei dati, il trattamento ulteriore dei dati personali per scopi statistici può avere come risultato solo dati aggregati che non possono essere riapplicati agli individui;

I Big Data a fini di contrasto

Privacy e protezione dei dati

25. rammenta a tutti i soggetti responsabili delle attività di contrasto che ricorrono al trattamento e all'analisi dei dati che la direttiva (UE) 2016/680: disciplina il trattamento dei dati personali da parte degli Stati membri ai fini delle attività di contrasto; esige che la raccolta e il trattamento dei dati personali ai fini di contrasto sia sempre adeguato, pertinente e non eccessivo in relazione agli obiettivi specificati, espliciti e legittimi per i quali i dati sono trattati; indica che lo scopo e la necessità della raccolta di tali dati devono essere chiaramente dimostrati; stabilisce che qualsiasi decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato è vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte dei titolari del trattamento; invita la Commissione, il Comitato europeo per la protezione dei dati e le altre autorità

di controllo indipendenti a mettere a punto orientamenti, raccomandazioni e buone pratiche per specificare ulteriormente i criteri e le condizioni delle decisioni adottate sulla base della profilazione e dell'uso dei Big Data ai fini delle attività di contrasto;

26. sottolinea l'importanza di rispettare la direttiva (UE) 2016/680 per quanto riguarda lo svolgimento di audit e di valutazioni d'impatto preliminari che tengano conto delle preoccupazioni di ordine etico, al fine di valutare l'inclusività, la precisione e la qualità dei dati nonché di garantire che le persone interessate dalle decisioni e/o i soggetti coinvolti nei processi decisionali siano in grado di comprendere e contestare la raccolta o l'analisi, i modelli e le correlazioni e di evitare effetti nocivi su determinati gruppi di persone;

27. evidenzia che la fiducia dei cittadini nei servizi digitali può essere seriamente compromessa da attività governative di sorveglianza di massa e dall'accesso ingiustificato ai dati commerciali e ad altri dati personali da parte delle autorità di contrasto;

28. ricorda che la legislazione che consente alle autorità pubbliche di ottenere l'accesso in maniera generalizzata al contenuto delle comunicazioni elettroniche deve essere considerata come un pericolo per l'essenza del diritto fondamentale al rispetto della vita privata del singolo, come garantito dall'articolo 7 della Carta;

29. sottolinea la necessità di linee guida e sistemi da integrare nelle gare pubbliche per i modelli, gli strumenti e i programmi di trattamento dei dati basati sui Big Data per fini di contrasto, onde garantire che il codice sottostante possa essere e sia controllato dalle stesse autorità di contrasto prima dell'acquisto finale e possano esserne verificate l'idoneità, la correttezza e la sicurezza, tenendo presente che la trasparenza e la responsabilità sono limitate dal software proprietario; evidenzia che taluni modelli di polizia predittiva sono più rispettosi della privacy di altri, per esempio laddove le previsioni probabilistiche sono effettuate su luoghi o eventi e non su persone singole;

Sicurezza

30. pone l'accento sull'assoluta necessità di proteggere le banche dati delle autorità di contrasto da violazioni della sicurezza e dall'accesso illecito, dal momento che tale questione desta preoccupazione tra i cittadini; ritiene, pertanto, che per affrontare tali rischi è necessario una cooperazione concertata ed efficace tra le autorità incaricate di contrasto, il settore privato, i governi e le autorità di controllo della protezione dei dati indipendenti; insiste sulla necessità di garantire un'adeguata sicurezza dei dati personali, a norma del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680, nonché di ridurre al minimo le vulnerabilità attraverso la progettazione di banche dati protette e decentrate;

Non discriminazione

31. avverte che, a causa dell'intrusività delle decisioni e delle misure adottate dalle autorità di contrasto - anche tramite il trattamento dei dati e l'analisi dei dati - nella vita e nei diritti dei cittadini, è necessaria la massima cautela onde evitare discriminazioni illegittime e attacchi nei confronti di determinate persone o gruppi di persone definite sulla base dell'origine razziale, etnica, sociale o del colore della pelle, delle caratteristiche genetiche, della lingua, della religione o credo, dell'opinione politica o di

qualsiasi altra opinione, della proprietà, della nascita, della disabilità, dell'età, del genere, dell'espressione o dell'identità di genere, dell'orientamento sessuale, dello status di residenza, della salute o dell'appartenenza a una minoranza nazionale, il che è spesso oggetto di profilazione etnica o di attività di polizia a fini di contrasto più intense, nonché nei confronti di persone che risultano essere definite da caratteristiche particolari; chiede l'adeguata formazione dei responsabili in prima linea della raccolta di dati e di coloro che utilizzano le informazioni di intelligence provenienti dall'analisi dei dati;

32. chiede alle autorità di contrasto degli Stati membri che ricorrono all'analisi dei dati di mantenere i più elevati standard etici nell'analisi dei dati e di garantire l'intervento umano e l'assunzione di responsabilità nelle varie fasi del processo decisionale, non solo per valutare la rappresentatività, la precisione e la qualità dei dati, ma anche per stabilire l'adeguatezza di ogni decisione da adottare sulla base di tali informazioni;

o

o o

33. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione.