EUROPEAN DATA PROTECTION SUPERVISOR

Parere 3/2015

La grande opportunità dell'Europa

Raccomandazioni del GEPD sulle opzioni dell'UE per la riforma della protezione dei dati

EDPS

28 luglio 2015

Il 24 giugno 2015 le tre principali istituzioni dell'UE, il Parlamento europeo, il Consiglio e la Commissione europea, hanno avviato i negoziati, nel quadro della procedura di codecisione, sulla proposta di regolamento generale sulla protezione dei dati (RGPD), procedura nota come "consultazione a tre" o "trilogo" informale[1]. Il trilogo è basato sulla proposta della Commissione del gennaio 2012, sulla risoluzione legislativa del Parlamento del 12 marzo 2014 e sull'orientamento generale del Consiglio adottato il 15 giugno 2015[2]. Le tre istituzioni sono impegnate a esaminare il RGPD nell'ambito del più ampio pacchetto di riforma in materia di protezione dei dati, che comprende la proposta di direttiva relativa alle attività di polizia e giudiziarie. La procedura dovrebbe concludersi alla fine del 2015 e verosimilmente consentire l'adozione formale di entrambi gli strumenti all'inizio del 2016, cui farà seguito un periodo transitorio di due anni. [3]

Il Garante europeo della protezione dei dati (GEPD) è un'istituzione indipendente dell'UE che non fa parte del trilogo ma, ai sensi dell'articolo 41, paragrafo 2, del regolamento 45/2001, ha il compito di "garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, riguardo al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari", *e* "...di fornire alle istituzioni e agli organismi comunitari nonché agli interessati pareri su tutte le questioni relative al trattamento dei dati personali". *Il garante e il garante aggiunto sono stati nominati nel dicembre 2014 con il compito specifico di essere più costruttivi e proattivi, e nel marzo 2015 hanno pubblicato una strategia quinquennale in cui hanno definito in che modo intendevano attuare tale compito, nonché renderne conto[4].*

Il presente parere costituisce la prima tappa importante della strategia del Garante europeo della protezione dei dati. Basandosi sui dibattiti tenuti con le istituzioni dell'UE, gli Stati membri, la società civile, l'industria e altre parti interessate, il nostro parere si prefigge di aiutare i partecipanti al trilogo a pervenire in tempo al consenso richiesto e tratta il RGPD in due parti:

- *la visione del GEPD per norme in materia di protezione dei dati orientate al futuro, con esempi illustrativi delle nostre raccomandazioni; e*
- *un allegato ("Allegato al parere 3/2015: tabella comparativa dei testi del RGPD con la raccomandazione del GEPD") con una tabella a quattro colonne per confrontare, articolo per articolo, il testo del RGPD come adottato rispettivamente da Commissione, Parlamento e Consiglio, con la raccomandazione del GEPD.*

Il parere è pubblicato sul nostro sito web e tramite un'applicazione per dispositivi mobili. Nell'autunno 2015 verrà integrato con raccomandazioni sia per i considerando del RGPD sia sulla protezione dei dati nell'ambito delle attività di polizia e giudiziarie, dopo l'adozione da parte del Consiglio della sua posizione generale sulla direttiva.

Resta valido l'esaustivo parere del GEPD del marzo 2012 relativo al pacchetto di riforma proposto dalla Commissione. A distanza di tre anni, tuttavia, era necessario aggiornare il nostro parere per confrontarci in modo più diretto con le posizioni dei colegislatori, nonché offrire raccomandazioni specifiche. [5] *Il presente parere, come quello del 2012, è in linea con i pareri e le dichiarazioni del Gruppo di lavoro articolo 29, compresa l'"Appendice" adottata il 18 giugno intitolata "Core topics in the view of trilogue"*

(Argomenti fondamentali nell'ottica del trilogo), a cui il GEPD ha contribuito come membro a pieno titolo del Gruppo di lavoro[6].

Una rara opportunità: perché questa riforma è così importante

L'UE sta per concludere la maratona per la riforma delle norme in materia di dati personali. Il regolamento generale sulla protezione dei dati interesserà potenzialmente, per decenni a venire, la totalità delle persone nell'UE e delle organizzazioni nell'UE che trattano dati personali nonché le organizzazioni al di fuori dell'UE che trattano dati personali relativi a persone nell'UE[7]. Occorre agire ora per tutelare i diritti e le libertà fondamentali delle persone nella società futura basata sui dati.

Una protezione dei dati efficace conferisce potere al singolo e stimola aziende e autorità pubbliche responsabili. In questo settore le normative sono tecniche e complesse e richiedono la consulenza di esperti, in particolare delle autorità indipendenti preposte alla protezione dei dati, consapevoli delle sfide in termini di conformità. Il RGPD sarà probabilmente una delle normative che rimarrà più a lungo in vigore nell'Unione, perciò ora l'UE deve puntare a essere selettiva, concentrarsi sulle disposizioni che sono davvero necessarie ed evitare dettagli che potrebbero, come conseguenza involontaria, interferire indebitamente con le tecnologie future. I testi di ciascuna istituzione esaltano la chiarezza e la comprensibilità in materia di trattamento dei dati personali: il RGPD deve quindi trasformare tali parole in fatti dimostrandosi il più possibile conciso e semplice da comprendere.

Spetta al Parlamento e al Consiglio, in qualità di colegislatori, definire il testo giuridico definitivo, coadiuvati dalla Commissione, titolare del diritto di iniziativa legislativa e custode dei Trattati. Il GEPD non prende parte ai negoziati del "trilogo", ma è giuridicamente competente a fornire il proprio parere, in modo proattivo, in linea con il compito assegnato al momento della nomina al garante e al garante aggiunto, nonché con la recente strategia del GEPD. Il presente parere si fonda su oltre dieci anni di esperienza in materia di controllo del rispetto della protezione dei dati e di consulenza politica per contribuire a guidare le istituzioni verso un risultato che favorisca gli interessi delle persone.

La legislazione è l'arte del possibile. Ciascuna delle opzioni sul tavolo, vale a dire i rispettivi testi preferiti da Commissione, Parlamento e Consiglio, contiene molte disposizioni valide, ma può essere migliorata. Il risultato non sarà perfetto nella nostra ottica, ma ci proponiamo di sostenere le istituzioni nel conseguimento del miglior risultato possibile. È per questa ragione che le raccomandazioni rimangono entro i limiti dei tre testi. Siamo guidati da tre costanti preoccupazioni:

- più vantaggi per i cittadini,
- norme che funzionino nella pratica,
- norme che durino una generazione.

Il presente parere è un esercizio di trasparenza e responsabilità, principi duali che sono forse l'innovazione più rilevante del RGPD. La procedura del trilogo è ora più che mai oggetto di accresciuta attenzione. Le raccomandazioni del GEPD sono di pubblico dominio, e vorremmo esortare tutte le istituzioni dell'UE a prendere l'iniziativa e dare l'esempio, cosicché questa riforma legislativa sia frutto di un procedimento trasparente e non di un compromesso segreto.

L'UE ha bisogno di un nuovo accordo sulla protezione dei dati, di un capitolo nuovo. Il resto nel mondo sta seguendo con attenzione gli sviluppi in corso. La qualità della nuova normativa e il modo in cui interagisce con i sistemi giuridici e le tendenze che si osservano a livello mondiale rivestono un'importanza fondamentale. Con il presente parere il GEPD segnala di essere pronto e disponibile ad aiutare a garantire che l'UE sfrutti al massimo questa opportunità storica.

I. INDICE

1 Più vantaggi per i cittadini 1

1. DEFINIZIONI: CHIARIAMO COSA SI INTENDE PER INFORMAZIONI DI CARATTERE PERSONALE 1
2. TUTTE LE OPERAZIONI DI TRATTAMENTO DEI DATI DEVONO ESSERE *SIA* LECITE *SIA* GIUSTIFICATE 1
3. UN CONTROLLO PIÙ INDIPENDENTE E PIÙ AUTOREVOLE 2

2 Norme che funzionino nella pratica 2

1. EFFICACIA DELLE SALVAGUARDIE, NON DELLE PROCEDURE 3
2. UN MIGLIORE EQUILIBRIO TRA L'INTERESSE PUBBLICO E LA PROTEZIONE DEI DATI PERSONALI 3
3. DARE FIDUCIA E POTERE ALLE AUTORITÀ DI CONTROLLO 3

3 Norme che durino una generazione 4

1. PRASSI COMMERCIALI RESPONSABILI E TECNICHE INNOVATIVE 4
2. CONFERIRE POTERE ALLE PERSONE FISICHE 5
3. NORME A PROVA DI FUTURO 5

4 Lavoro incompiuto 5

5 Un momento importante per i diritti digitali in Europa e non solo 5

Note 7

1 Più vantaggi per i cittadini

Le norme dell'UE hanno sempre cercato di agevolare i flussi di dati, sia all'interno dell'UE che con i suoi partner commerciali, preoccupandosi comunque costantemente dei diritti e delle libertà delle persone. Internet ha permesso un grado senza precedenti di connessione, espressione personale e opportunità per offrire valore ad aziende e consumatori. Nondimeno, la vita privata è per gli europei più importante che mai. Secondo un sondaggio condotto dall'Eurobarometro nel giugno 2015 in materia di protezione dei dati[8], oltre sei cittadini su dieci non si fidano delle imprese operanti online e due terzi si preoccupano di non avere pieno controllo sui dati che forniscono online.

La riforma del quadro di regolamentazione deve mantenere e, ove possibile, innalzare gli standard a vantaggio delle persone. Il pacchetto di riforma della protezione dei dati è stato proposto prima di tutto come veicolo per "rafforzare i diritti della privacy on line" garantendo che le persone siano più informate sui propri diritti e abbiano un maggiore controllo dei propri dati[9]. Nell'aprile 2015 i rappresentanti delle organizzazioni della società civile hanno scritto alla Commissione europea per esortare le istituzioni a tener fede a queste intenzioni[10].

I principi esistenti stabiliti nella Carta, fonte di diritto primario dell'UE, dovrebbero essere applicati in modo coerente, dinamico e innovativo così da renderli efficaci per i cittadini nella pratica. La riforma deve essere globale, da qui l'impegno per un pacchetto, ma poiché è probabile che il trattamento dei dati venga disciplinato da strumenti giuridici distinti occorre che vi sia chiarezza sul loro specifico campo d'applicazione e sul modo in cui funzionano congiuntamente, senza scappatoie per trovare compromessi sulle salvaguardie[11].

Per il GEPD, il punto di partenza è la dignità della persona, che trascende le questioni di mera conformità giuridica[12]. Le nostre raccomandazioni si fondano su una valutazione di ciascun articolo del RGPD, singolarmente e cumulativamente, in funzione della sua capacità di rafforzare la posizione della persona rispetto al quadro attuale. Punto di riferimento sono i principi fulcro della protezione di dati, vale a dire l'articolo 8 della Carta dei diritti fondamentali[13].

1. Definizioni: chiariamo cosa si intende per informazioni di carattere personale

- Le persone dovrebbero poter esercitare con più efficacia i propri diritti relativamente a qualsiasi informazione che può renderle identificabili o individuabili, anche se tali informazioni si ritengono "pseudonimizzate"[14].

2. Tutte le operazioni di trattamento dei dati devono essere *sia* lecite *sia* giustificate

- Gli obblighi per cui tutte le operazioni di trattamento dei dati devono essere limitate a finalità specifiche e avere una base giuridica sono cumulativi, non alternativi. Raccomandiamo di evitare qualsiasi fusione e un conseguente indebolimento di tali principi. L'UE dovrebbe piuttosto preservare, semplificare e rendere operativa la nozione consolidata per cui i dati di carattere personale

dovrebbero essere usati solo in modi compatibili con le finalità di raccolta originali[15].

- Il consenso è una delle possibili basi giuridiche per il trattamento, ma occorre evitare l'uso di caselle da spuntare obbligatoriamente laddove non esiste una scelta significativa per l'individuo e il trattamento dei dati non è necessario. Si raccomanda di dare modo alle persone di fornire un consenso ampio o limitato, ad esempio alla ricerca in ambito clinico, che venga rispettato e che possa essere revocato[16].

- Il GEPD sostiene soluzioni valide e innovative per i trasferimenti internazionali di informazioni personali che agevolano gli scambi di dati e rispettano i principi in materia di protezione e controllo dei dati. Consigliamo vivamente di non permettere i trasferimenti sulla base dei legittimi interessi del responsabile del trattamento per via dell'insufficiente protezione delle persone fisiche, né l'UE dovrebbe consentire il libero accesso da parte di autorità di paesi terzi a dati che si trovano nell'UE. Qualsiasi richiesta di trasferimento presentata da autorità di un paese terzo dovrebbe essere riconosciuta soltanto qualora rispetti le norme stabilite nei trattati di mutua assistenza giudiziaria, negli accordi internazionali o in altri canali giuridici per la cooperazione internazionale[17].

3. Un controllo più indipendente e più autorevole

- Le autorità competenti per la protezione dei dati personali dell'UE dovrebbero essere pronte a esercitare il proprio ruolo nel momento in cui il RGPD entrerà in vigore, con la piena operatività del comitato per la protezione dei dati non appena il regolamento diventerà applicabile[18].

- Le autorità dovrebbero essere in grado di ricevere ed esaminare i reclami e le denunce presentate da qualsiasi interessato o organismo, organizzazione e associazione.

- Il rispetto dei diritti delle persone richiede un sistema di responsabilità e risarcimento efficace per i danni causati dal trattamento illecito dei dati. Dati gli evidenti ostacoli per ottenere riparazione nella pratica, in sede giudiziale le persone fisiche dovrebbero poter essere rappresentate da organismi, organizzazioni e associazioni[19].

2 Norme che funzionino nella pratica

Le salvaguardie non dovrebbero essere confuse con le formalità. Troppi dettagli o tentativi di microgestione dei processi aziendali rischiano in futuro di diventare antiquati. Qui possiamo prendere spunto dal manuale sulla concorrenza dell'UE, dove un corpus di diritto derivato relativamente limitato viene applicato in modo rigoroso e incoraggia una cultura improntata alla responsabilità e alla consapevolezza tra le imprese[20].

Ciascuno dei tre testi pretende dai responsabili del trattamento delle informazioni di carattere personale maggiore chiarezza e semplicità[21]. Allo stesso modo anche gli obblighi tecnici devono essere concisi e di facile comprensione per essere attuati dai responsabili del trattamento in modo adeguato[22].

Le procedure esistenti non sono inviolabili: le nostre raccomandazioni si prefiggono di individuare possibilità di deburocratizzazione, riducendo al minimo le prescrizioni per la documentazione e le formalità prive di importanza. Raccomandiamo di legiferare solo laddove veramente necessario, offrendo così spazio di manovra ad aziende, autorità pubbliche o autorità competenti per la protezione dei dati personali: uno spazio che deve essere colmato con la responsabilizzazione e gli orientamenti forniti da queste ultime autorità. Nel complesso, le nostre raccomandazioni produrrebbero un testo del RGPD più breve quasi del 30 % rispetto alla lunghezza media dei testi delle tre istituzioni[23].

1. Efficacia delle salvaguardie, non delle procedure

- Nell'ottica del rispetto della normativa, la documentazione dovrebbe essere un mezzo e non un fine; la riforma deve concentrarsi sui risultati. Raccomandiamo un approccio scalabile che riduca gli obblighi dei responsabili del trattamento in termini di documentazione a un'unica politica riguardante la conformità al regolamento tenendo conto dei rischi, con una dimostrazione trasparente di tale conformità, sia essa relativa a trasferimenti, contratti con gli incaricati del trattamento o notificazioni delle violazioni[24].

- Sulla base di espliciti criteri per la valutazione dei rischi, e forti della nostra esperienza di controllo delle istituzioni dell'UE, raccomandiamo di richiedere la notificazione di violazione dei dati all'autorità di controllo e le valutazioni d'impatto sulla protezione dei dati solo laddove i diritti e le libertà degli interessati sono a rischio[25].

- Le iniziative dell'industria, che siano tramite norme vincolanti d'impresa o sigilli di protezione dei dati, dovrebbero essere incoraggiate attivamente[26].

2. Un migliore equilibrio tra l'interesse pubblico e la protezione dei dati personali

- Le norme in materia di protezione dei dati non dovrebbero ostacolare il trattamento per finalità storiche, statistiche e di ricerca scientifica che siano realmente di interesse pubblico. I responsabili devono adottare le disposizioni necessarie per impedire che le informazioni personali vengano usate contro l'interesse della persona, per esempio prestando particolare attenzione alle norme che disciplinano le informazioni sensibili relative alla salute[27].

- I ricercatori e gli archivisti dovrebbero avere la facoltà di conservare i dati fintantoché questo risulti necessario, purché nel rispetto di tali salvaguardie[28].

3. Dare fiducia e potere alle autorità di controllo

- Raccomandiamo di permettere alle autorità di controllo di fornire orientamenti ai responsabili del trattamento e di sviluppare le proprie norme procedurali interne nello spirito di un'applicazione semplificata e più semplice del RGPD da parte di un'unica autorità di controllo (lo "sportello unico") vicina al cittadino ("prossimità"). [29]

- Le autorità dovrebbero avere la facoltà di stabilire sanzioni riparatorie e amministrative efficaci, proporzionate e dissuasive sulla base di tutte le circostanze pertinenti[30].

3 Norme che durino una generazione

Il principale pilastro del quadro normativo attuale, la direttiva 95/46/CE, ha rappresentato un modello per l'ulteriore legislazione in materia di trattamento dei dati nell'UE e nel mondo, e ha persino fornito le basi per la formulazione del diritto alla protezione dei dati di carattere personale di cui all'articolo 8 della Carta dei diritti fondamentali. La presente riforma inciderà profondamente sul trattamento dei dati per una generazione che non ha memoria di una vita senza Internet. L'UE deve pertanto comprendere a pieno le implicazioni che questo atto comporta per le persone, nonché la sua sostenibilità di fronte allo sviluppo tecnologico.

Negli ultimi anni si è assistito a un incremento esponenziale in termini di generazione, raccolta, analisi e scambio di informazioni personali, il risultato di innovazioni tecnologiche come l'Internet degli oggetti, il cloud computing, i megadati e i dati aperti, il cui sfruttamento è ritenuto fondamentale dall'UE per la sua competitività[31]. A giudicare dalla longevità della direttiva 95/46/CE, è ragionevole aspettarsi che occorra un lasso di tempo analogo prima della prossima importante revisione delle norme in materia di protezione dei dati, che forse non avverrà prima della fine degli anni 2030. Molto prima di allora è possibile ritenere che le tecnologie guidate dai dati siano state fatte convergere con l'intelligenza artificiale, l'elaborazione del linguaggio naturale e i sistemi biometrici, conferendo alle applicazioni capaci di apprendimento automatico un'intelligenza avanzata.

Queste tecnologie stanno sfidando i principi della protezione dei dati. Una riforma orientata al futuro deve pertanto essere incentrata sulla dignità della persona e improntata all'etica. Deve compensare lo squilibrio tra l'innovazione nella protezione dei dati personali e il suo sfruttamento, rendendo le salvaguardie efficaci nella nostra società digitalizzata.

1. Prassi commerciali responsabili e tecniche innovative

- La riforma dovrebbe invertire le recenti tendenze orientate al tracciamento segreto e a un processo decisionale sulla base di profili nascosti alle persone. Il problema non è la pubblicità mirata o la prassi di tracciare profili ("profiling"), ma piuttosto la mancanza di informazioni significative sull'algoritmo logico che sviluppa tali profili e incide sugli interessati[32]. Raccomandiamo una maggiore trasparenza da parte dei responsabili del trattamento.

- Sosteniamo pienamente l'introduzione dei principi della protezione fin dalla progettazione e della protezione di default come mezzi per ridare impulso alle soluzioni guidate dal mercato nell'economia digitale. Raccomandiamo una formulazione più semplice perché i diritti e gli interessi della persona fisica siano integrati nello sviluppo dei prodotti e nelle impostazioni di default[33].

2. Conferire potere alle persone fisiche

- La portabilità dei dati nell'ambiente digitale è la via che conduce al controllo da parte dell'utente, che le persone si stanno accorgendo di non avere. Raccomandiamo di permettere un trasferimento diretto dei dati da un responsabile del trattamento a un altro su richiesta dell'interessato e di dare a quest'ultimo il diritto di ricevere una copia dei dati che lui stesso può trasferire a un altro responsabile del trattamento[34].

3. Norme a prova di futuro

- Raccomandiamo di evitare un linguaggio e delle prassi che possano diventare datati o discutibili[35].

4 Lavoro incompiuto

L'adozione di un pacchetto di riforma della protezione dei dati nell'UE orientato al futuro sarà un risultato notevole, ma nondimeno incompleto.

Tutte le istituzioni convengono sul fatto che i principi del RGPD dovrebbero applicarsi alle istituzioni dell'UE in modo coerente. Abbiamo sostenuto la certezza del diritto e l'uniformità del quadro giuridico, accettando al contempo l'unicità del settore pubblico dell'UE e la necessità di evitare qualsiasi indebolimento del livello di obblighi attuale (nonché il bisogno di fornire la base giuridica e organizzativa per il GEPD). La Commissione dovrebbe pertanto presentare una proposta coerente con il RGPD per la revisione del regolamento 45/2001 non appena possibile una volta concluse le trattative sul RGPD, così che entrambi i testi possano diventare applicabili contemporaneamente[36].

In secondo luogo, risulta chiaro che la direttiva 2002/58/CE (la direttiva "e-privacy") dovrà essere modificata. Aspetto molto più rilevante è che all'UE occorre un quadro legislativo chiaro per la riservatezza delle comunicazioni, un elemento necessario del rispetto della vita privata, che disciplini tutti i servizi che permettono le comunicazioni, non soltanto i fornitori di comunicazioni elettroniche accessibili al pubblico. Ciò deve essere realizzato per mezzo di un regolamento giuridicamente certo e di armonizzazione che fornisca almeno gli stessi standard di protezione di cui alla direttiva e-privacy a parità di condizioni.

Il presente parere raccomanda pertanto di esigere il prima possibile un impegno per la rapida adozione di proposte in questi due settori.

5 Un momento importante per i diritti digitali in Europa e non solo

Per la prima volta in una generazione, l'UE ha l'opportunità di modernizzare e armonizzare le norme sulle modalità di trattamento delle informazioni personali. Il rispetto della vita privata e la protezione dei dati non sono in concorrenza con la crescita economica e il commercio internazionale, né con servizi e prodotti validi; fanno parte di una proposta orientata a qualità e valore. Come riconosce il Consiglio europeo, la fiducia è un requisito indispensabile per prodotti e servizi innovativi che fanno affidamento sul trattamento dei dati personali.

In materia di protezione dei dati nel 1995 l'UE era all'avanguardia. Ora oltre 100 paesi in tutto il mondo hanno una normativa in materia di protezione dei dati e meno della metà di questi sono paesi europei[37]. Ciononostante l'UE continua a essere osservata con molta attenzione da quei paesi che stanno considerando di attuare o rivedere i propri quadri giuridici. In un momento in cui la fiducia delle persone in aziende e governi è stata minata da rivelazioni sulla sorveglianza di massa e sulle violazioni di dati, questo conferisce una notevole responsabilità ai legislatori dell'UE le cui decisioni di quest'anno avranno un impatto oltre i confini dell'Europa.

Nell'ottica del GEPD, i testi del RGPD sono sulla strada giusta, ma permangono preoccupazioni, alcune molto gravi. Con la procedura di codecisione sussiste sempre un rischio che determinate disposizioni vengano indebolite da negoziatori armati di buone intenzioni in cerca di un compromesso politico. Con la riforma sulla protezione dei dati è tuttavia diverso, perché abbiamo a che fare con diritti fondamentali e il modo in cui verranno salvaguardati per una generazione.

Su tale base, il presente parere intende aiutare le principali istituzioni dell'UE a risolvere i problemi. Non vogliamo solo diritti più forti per il singolo interessato e una maggiore responsabilità per il responsabile del trattamento; vogliamo agevolare l'innovazione con un quadro giuridico che sia neutrale nei confronti della tecnologia ma fiducioso rispetto ai vantaggi che questa può apportare alla società.

Ora che i negoziati sono quasi conclusi, speriamo che le nostre raccomandazioni aiutino l'UE a raggiungere il traguardo con una riforma che resti idonea allo scopo negli anni e decenni a venire: un nuovo capitolo per la protezione dei dati con una prospettiva globale, in cui l'UE si pone alla guida dando l'esempio.

Bruxelles, 28 luglio 2015

Giovanni BUTTARELLI

Garante europeo della protezione dei dati

Addendum

In data 27 luglio 2015 abbiamo pubblicato (parere del GEPD 3/2015) le nostre raccomandazioni redazionali per le disposizioni operative del RGPD. Dopo aver riflettuto sui principi alla base degli articoli nelle tre versioni adottate, rispettivamente, dalla Commissione, dal Parlamento europeo e dal Consiglio, teniamo a proporre, come ulteriore contributo ai negoziati del trilogo in corso, le nostre raccomandazioni relative al contenuto dei considerando del RGPD.

I considerando nel preambolo di uno strumento giuridico dell'UE sono importanti perché spiegano i motivi alla base di ciascuna disposizione. Sebbene privi di valore giuridico autonomo, i considerando possono essere utilizzati nell'interpretazione del campo di applicazione delle disposizioni sostanziali nel testo. La CGUE ha dichiarato in diverse occasioni che alla Corte sono necessari considerando validi per svolgere la sua funzione di interpretazione della legge. Poiché forniscono le motivazioni alla base dell'atto giuridico, essi meritano attenta considerazione.

Di conseguenza, in queste raccomandazioni, ribadiamo che il rispetto per la dignità umana dovrebbe essere affermato quale base per ogni trattamento di dati personali. Il RGPD deve servire come modello per un approccio etico attento ai benefici sociali apportati da cambiamenti e innovazioni di tipo tecnologico, che tuteli al contempo le persone fisiche, fornendo loro i mezzi per avere il controllo dei propri dati nel cyberspazio. I considerando dovrebbero promuovere ulteriormente la rendicontabilità dei responsabili del trattamento e lasciare maggiore spazio agli orientamenti forniti dalle autorità di controllo all'interno del Comitato europeo per la protezione dei dati.

Continuiamo ad incoraggiare proposte redazionali il più possibile chiare, concise e comprensibili. Le nostre raccomandazioni eliminerebbero, inoltre, dai considerando ogni dettaglio non necessario, che potrebbe limitare la flessibilità indispensabile per adattarsi alle sfide future, in un'epoca dove i cambiamenti rapidi costituiscono la nuova norma.

Bruxelles, 9 ottobre 2015

Giovanni Buttarelli

Note

[1] Dichiarazioni comuni Parlamento europeo, Consiglio, Commissione - Dichiarazione comune sulle modalità pratiche della procedura di codecisione (articolo 251 del trattato CE) (2007/C 145/02), GU C 145 del 30.6.2007.

[2] COM(2012)11 final; risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), P7_TA(2014)0212; proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) - Elaborazione di un orientamento generale, documento del Consiglio 9565/15 dell'11 giugno 2015.

[3] Il titolo completo è: Proposta di direttiva concernente la tutela 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, e la libera circolazione di tali dati, COM(2012)10 final; risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela 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, e la libera circolazione di tali dati, P7_TA(2014)0219. Per la tempistica e la portata del trilogo, cfr. le conclusioni del Consiglio europeo del 25-26 giugno 2015, EUCO 22/15; una "tabella di marcia" per il trilogo è stata indicata in occasione di una conferenza stampa congiunta di Parlamento, Consiglio e Commissione http://audiovisual.europarl.europa.eu/AssetDetail.aspx?id=690e8d8d-682d-4755-bfb6-a4c100eda4ed [ultimo accesso: 20.7.2015], ma non è stata pubblicata ufficialmente. Il RGPD entrerà in vigore 20 giorni dopo la sua pubblicazione nella Gazzetta ufficiale e si ritiene che sarà pienamente applicabile due anni dopo la sua entrata in vigore (articolo 91).

[4] Posto vacante di garante europeo della protezione dei dati COM/2014/10354 (2014/C 163 A/02), GU C 163 A/6 del 28.5.2014. La strategia 2015-2019 del GEPD ha promesso di "cercare soluzioni attuabili che evitino un appesantimento burocratico, rimangano flessibili per l'innovazione tecnologica e i flussi di dati transfrontalieri e consentano alle persone di esercitare i propri diritti più efficacemente online e offline"; Leading by example: The EDPS Strategy 2015-2019, marzo 2015.

[5] Parere del GEPD del 7 marzo 2012 sul pacchetto di riforma della protezione dei dati.

[6] Cfr. l'allegato alla Lettera del Gruppo di lavoro dell'articolo 29 a Věra Jourová, commissaria per la giustizia, i consumatori e la parità di genere, del 17.6.2015.

[7] Il campo di applicazione materiale e territoriale del RGPD è difficile da riassumere in modo conciso. Le istituzioni sembrano almeno convenire sul fatto che comprende le organizzazioni con sede all'interno dell'UE che sono responsabili del trattamento di dati personali all'interno o all'esterno dell'UE, le organizzazioni con sede al di fuori dell'UE che trattano dati personali di persone nell'UE nel corso di attività di offerta di prodotti o servizi o di monitoraggio di persone nell'UE (cfr. l'articolo 2 sul campo di applicazione materiale e l'articolo 3 sul campo di applicazione territoriale).

[8] Altri risultati indicano che sette persone su dieci sono preoccupate del fatto che i loro dati vengano usati per finalità diverse da quelle per cui erano stati raccolti, una persona su sette sottolinea che in tutti i casi dovrebbe essere richiesta l'esplicita autorizzazione dell'interessato prima della raccolta e del trattamento dei dati, e due terzi ritengono importante avere la facoltà di trasferire informazioni personali da un prestatore di servizi precedente a uno nuovo;

Eurobarometro speciale 431 sulla protezione dei dati, giugno 2015. Risultati comparabili ottenuti da Pew Research nel 2014 indicano che il 91 % degli americani sente di aver perso il controllo sul modo in cui le aziende raccolgono e utilizzano le informazioni personali, l'80 % degli utenti dei social network è preoccupato del fatto che i loro dati finiscono nelle mani di terzi quali inserzionisti o aziende e il 64 % afferma che il governo dovrebbe fare di più per regolamentare il comportamento degli inserzionisti; Privacy Panel Survey, Pew Research, gennaio 2014.

[9] La Commissione propone una riforma generale delle norme in materia di protezione dei dati per aumentare il controllo degli utenti sui propri dati e tagliare i costi per le imprese.

[10] Lettera delle ONG al presidente Juncker, 21.4.2015 https://edri.org/files/DP_letter_Juncker_20150421.pdf e risposta del capo di gabinetto del vicepresidente Timmermans, 17.7.2015 https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf [ultimo accesso: 23.7.2015]. Nel maggio 2015 il GEPD ha incontrato i rappresentanti di alcune di queste ONG per discutere le loro preoccupazioni: Comunicato stampa EDPS/2015/04, 1.6.2015, EU Data Protection Reform: the EDPS meets international civil liberties groups; la registrazione completa del dibattito è disponibile sul sito web del GEPD (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Videos/GDPR_civil_soc).

[11] Articolo 2, paragrafo 2, lettera e).

[12] Articolo 1.

[13] L'articolo 8 della Carta dispone che [grassetto aggiunto]:

> *1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*
>
> *2. Tali dati devono essere* ***trattati secondo il principio di lealtà****, per* ***finalità determinate*** *e* ***in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge.*** *Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e* ***di ottenerne la rettifica****.*
>
> *3. Il rispetto di tali regole è soggetto al* ***controllo di un'autorità indipendente.***

[14] Articolo 10. A meno che esista e fino a quando non vi sarà una definizione chiara e giuridicamente vincolante per "dati pseudonimizzati" che li distingua dai "dati di carattere personale", questo tipo di dati deve rimanere nel campo di applicazione delle norme in materia di protezione dei dati.

[15] Articolo 6, paragrafi 2 e 4. Dato che vi è stata qualche incertezza sul significato di "compatibilità" raccomandiamo, seguendo il parere del gruppo dell'articolo 29 sulla limitazione delle finalità, criteri generali per valutare se il trattamento sia compatibile (cfr. l'articolo 5, paragrafo 2).

[16] Un'effettiva separazione funzionale è un mezzo per garantire un trattamento lecito in assenza di consenso, ma l'interesse legittimo non dovrebbe essere oggetto di eccessiva interpretazione. In alcune situazioni anche un diritto incondizionato di dissociarsi può essere un'alternativa adeguata. La valutazione di una libera manifestazione di consenso dipende in parte da (a) l'esistenza di un notevole squilibrio tra l'interessato e il responsabile del trattamento e (b) il fatto che l'esecuzione di un contratto o la fornitura di un servizio, nei casi di trattamento di cui all'articolo 6, paragrafo 1, lettera b), sia stata realizzata subordinatamente a un consenso al trattamento dei dati non necessario per tali finalità (cfr. l'articolo 7, paragrafo 4). Questo rispecchia quanto previsto nella normativa dell'UE relativa al diritto dei consumatori: ai sensi dell'articolo 3, paragrafo 1, della direttiva 93/13/CEE del 5 aprile 1993 concernente le clausole abusive nei contratti stipulati con i consumatori: "Una clausola contrattuale, che non è stata oggetto di negoziato individuale, si considera abusiva se, malgrado il requisito della buona fede, determina, a danno del consumatore, un significativo squilibrio dei diritti e degli obblighi delle parti derivanti dal contratto".

[17] Tali norme includono le decisioni in materia di adeguatezza per settori e territori specifici, le verifiche periodiche delle decisioni di adeguatezza e le norme vincolanti di impresa. Cfr. gli articoli 40-45.

[18] Articolo 73.

[19] Articolo 76. Per quanto concerne la difficoltà nell'ottenere riparazione per violazione delle norme in materia di protezione dei dati, cfr. la relazione dell'Agenzia per i diritti fondamentali, Accesso ai mezzi di ricorso per la protezione dei dati negli Stati membri dell'Unione europea, 2013.

[20] Le norme dell'UE pongono particolare accento sull'autovalutazione da parte delle aziende per quanto riguarda il rispetto dell'articolo 101 del TFUE, divieto di accordi che siano restrittivi della concorrenza, mentre le imprese dominanti in un mercato hanno una "responsabilità speciale" di evitare qualsiasi azione che potrebbe ostacolare una concorrenza effettiva (paragrafo 9 degli orientamenti della Commissione, 2009/C 45/02); cfr. parere preliminare del Garante europeo della protezione dei dati su vita privata e competitività nell'era dei megadati, 14.3.2014.

[21] I tre testi fanno riferimento in vario modo alla necessità di comunicare "in modo e forma [...] intelligibili usando una formulazione chiara e semplice" (considerando 57, PE; articolo 19, COM e Consiglio), a diritti "chiari e inequivocabili" (considerando 99, PE; articolo 10 *bis* PE) e alla fornitura di "informazioni chiare e di facile comprensione" (articolo 10 PE, articolo 11 PE) e di informazioni che siano "concise, trasparenti, chiare e facilmente accessibili" (considerando 25, PE, COM e Consiglio; articolo 11 PE).

[22] Nelle versioni del Parlamento e del Consiglio le disposizioni inerenti agli atti delegati sono state in larga parte eliminate. Crediamo che l'UE possa andare oltre e lasciare tali questioni tecniche alla competenza di autorità indipendenti.

[23] Le nostre raccomandazioni produrrebbero un testo di circa 20 000 parole; la lunghezza media dei testi delle tre istituzioni si attesta intorno alle 28 000 parole.

[24] Articolo 22.

[25] Articoli 31 e 33.

[26] Articolo 39.

[27] Articolo 83. La ricerca e l'archiviazione di per se stesse non costituiscono una base giuridica per il trattamento, ragione per cui raccomandiamo l'eliminazione dell'articolo 6, paragrafo 2.

[28] Articolo 83 *bis*.

[29] Il gruppo dell'articolo 29 ha delineato una visione di governance, il meccanismo di coerenza e lo sportello unico basati sulla fiducia nei confronti delle autorità competenti per la protezione dei dati personali indipendenti e formulati su tre livelli:

- la singola autorità competente per la protezione dei dati personali, forte e pienamente in grado di trattare casi che rientrano nella sua sfera di competenza;
- una cooperazione efficace tra le autorità competenti per la protezione dei dati personali, con una chiara autorità capofila per i casi transfrontalieri;
- il comitato europeo per la protezione dei dati, che deve essere autonomo, dotato di personalità giuridica propria, fornito di mezzi sufficienti, composto da autorità competenti per la protezione dei dati personali alla pari che operano in uno spirito di solidarietà, con la facoltà di prendere decisioni vincolanti e coadiuvato da una segreteria che presta i propri servizi al comitato tramite la presidenza.

[30] Raccomandiamo inoltre di chiarire la competenza delle autorità di controllo e la nomina di un'autorità capofila nei casi di trattamento transnazionali, preservando al contempo la facoltà

delle autorità di controllo di gestire casi puramente locali. Raccomandiamo una versione semplificata del meccanismo di coerenza che faccia maggiore chiarezza su come individuare i casi in cui le autorità di controllo avrebbero bisogno di consultare il comitato europeo per la protezione dei dati e in cui il comitato dovrebbe adottare una decisione vincolante al fine di garantire la coerente applicazione del regolamento.

[31] Comunicazione della Commissione, Strategia per il mercato unico digitale in Europa, COM(2015) 192 final; Conclusioni del Consiglio europeo del giugno 2015, EUCO 22/15; Conclusioni del Consiglio sulla trasformazione digitale dell'industria europea, 8993/15.

[32] Articolo 14, lettera h).

[33] Articolo 23.

[34] Articolo 18. Raccomandiamo inoltre che, perché sia efficace, il diritto alla portabilità dei dati debba avere un ampio campo d'applicazione, e non essere applicato soltanto alle operazioni di trattamento che usano i dati forniti dall'interessato.

[35] Consigliamo, per esempio, di omettere espressioni quali "online", "per iscritto" e "la società dell'informazione".

[36] Una possibilità, da noi preferita, è che questo venga effettuato per mezzo di una disposizione nel RGPD stesso.

[37] Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority (30 gennaio 2015), a cura di Graham Greenleaf; (2015) 133 Privacy Laws & Business International Report, febbraio 2015; documento di ricerca in diritto n. 2015-21 a cura dell'UNSW.