I

(Risoluzioni, raccomandazioni e pareri)

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del Garante europeo della protezione dei datisulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — «Un approccio globale alla protezione dei dati personali nell'Unione europea»

(2011/C 181/01)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 7 e 8,

vista la 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 [1],

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati [2], in particolare l'articolo 41,

HA ADOTTATO IL SEGUENTE PARERE:

A. **PARTE GENERALE**

1. **Introduzione**

1.1. *Una prima e generale valutazione*

1. Il 4 novembre 2010 la Commissione ha adottato una comunicazione dal titolo «Un approccio globale alla protezione dei dati personali nell'Unione europea» (la «comunicazione») [3]. La comunicazione è stata trasmessa al GEPD per consultazione. Il GEPD si compiace di essere stato consultato dalla Commissione conformemente all'articolo 41 del regolamento (CE) n. 45/2001. Già prima dell'adozione della comunicazione il GEPD aveva avuto la possibilità di formulare osservazioni informali, alcune delle quali sono state prese in considerazione nella versione definitiva del documento.

2. Obiettivo della comunicazione è definire l'approccio della Commissione per rivedere il quadro giuridico dell'UE che disciplina la protezione dei dati personali in tutti i settori di attività dell'Unione, tenendo conto in particolare delle sfide generate dalla globalizzazione e dalle nuove tecnologie [4].

3. Il GEPD accoglie con favore la comunicazione in generale, poiché è convinto che sia necessario rivedere l'attuale quadro giuridico sulla protezione dei dati nell'UE al fine di garantire una tutela efficace in una società dell'informazione destinata a svilupparsi ulteriormente. Già nel parere formulato il 25 luglio 2007 sull'applicazione della direttiva sulla protezione dei dati [5] il GEPD aveva concluso che, a più lungo termine, delle modifiche della direttiva 95/46/CE sarebbero state inevitabili.

4. La comunicazione rappresenta un considerevole passo avanti verso tale cambiamento normativo, che a sua volta costituirà lo sviluppo più importante nel settore della protezione dei dati dell'UE dall'adozione della direttiva 95/46/CE, che viene generalmente considerata la principale pietra miliare della protezione dei dati nell'Unione europea (e, a livello più ampio, nello Spazio economico europeo).

5. La comunicazione fornisce il quadro adeguato per una revisione mirata, anche perché individua — generalmente parlando — le questioni e le sfide principali. Il GEPD condivide il parere della Commissione secondo cui in futuro continuerà a essere necessario disporre di un solido sistema di protezione dei dati, partendo dal presupposto che gli attuali principi generali di protezione dei dati continueranno a rimanere validi in una società che è sottoposta a profonde trasformazioni a causa dei rapidi sviluppi tecnologici e della globalizzazione. È pertanto necessaria una revisione delle misure legislative esistenti.

[1] GU L 281 del 23.11.1995, pag. 31.
[2] GU L 8 del 12.1.2001, pag. 1.
[3] COM(2010) 609 definitivo.
[4] Cfr. la pagina 5 della comunicazione, primo paragrafo.
[5] Parere del GEPD del 25 luglio 2007 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati, (GU C 255 del 27.10.2007, pag. 1).

6. La comunicazione sottolinea giustamente che le sfide sono enormi. Il GEPD condivide appieno tale affermazione e sottolinea che, di conseguenza, le soluzioni proposte devono essere altrettanto ambiziose e rafforzare l'efficacia della protezione.

1.2. *Obiettivo del parere*

7. Il presente parere valuta le soluzioni proposte nella comunicazione sulla base di questi due criteri: ambizione ed efficacia. In generale la prospettiva è positiva. Il GEPD sostiene la comunicazione, ma al tempo stesso esprime una posizione critica su aspetti in cui, a suo parere, una maggiore ambizione darebbe luogo a un sistema più efficace.

8. Con il presente parere il GEPD intende contribuire all'ulteriore sviluppo del quadro giuridico per la protezione dei dati. Il GEPD attende la proposta della Commissione prevista per la metà del 2011 e auspica che i suoi suggerimenti vengano presi in considerazione nella formulazione della proposta. Osserva inoltre che la comunicazione sembra escludere dallo strumento generale taluni settori, quali il trattamento dei dati da parte delle istituzioni e degli organismi dell'UE. Il GEPD esorta la Commissione — nel caso in cui quest'ultima dovesse effettivamente decidere di tralasciare determinati settori in questa fase, scelta che peraltro il GEPD troverebbe non condivisibile — a impegnarsi a realizzare un'architettura organica in tempi brevi e precisi.

1.3. *I capisaldi del parere*

9. Il presente parere non va considerato in maniera isolata. Esso si basa infatti su posizioni precedentemente espresse dal GEPD e dalle autorità europee di protezione dei dati in varie occasioni. In particolare è opportuno sottolineare che nel summenzionato parere del GEPD del 25 luglio 2007 sono stati individuati e sviluppati alcuni elementi principali delle future modifiche ([6]). Questo parere si basa inoltre sulle discussioni intercorse con altre parti interessate nei settori della protezione dei dati e della vita privata. Grazie al loro contributo è stato possibile ottenere informazioni di base molto utili sia per la comunicazione sia per il presente parere. A tale proposito si può concludere che esiste una certa sinergia sulle modalità di miglioramento dell'efficacia della protezione dei dati.

10. Un altro importante caposaldo del presente parere è il documento intitolato «The future of privacy» (Il futuro della privacy), contributo congiunto del Gruppo di lavoro articolo 29 per la protezione dei dati e del Gruppo di lavoro «polizia e giustizia» alla consultazione lanciata dalla Commissione nel 2009 (il «documento del Gruppo di lavoro sul futuro della privacy») ([7]).

11. Più di recente, in occasione di una conferenza stampa svoltasi il 15 novembre 2010, il GEPD ha espresso le sue prime considerazioni sulla comunicazione. Il presente parere approfondisce le opinioni più generali formulate nel corso di tale conferenza stampa ([8]).

12. Infine, il presente parere si basa su una serie di pareri precedenti del GEPD nonché su documenti del Gruppo di lavoro articolo 29 per la protezione dei dati. A tali pareri e documenti viene fatto riferimento, se del caso, in vari punti del presente parere.

2. **Contesto**

13. La revisione delle norme di protezione dei dati avviene in un momento storico cruciale. La comunicazione descrive il contesto in maniera approfondita e convincente. Sulla base di tale descrizione il GEPD individua i quattro fattori principali che determinano l'ambiente in cui avviene il processo di revisione.

14. Il primo fattore è lo sviluppo tecnologico. La tecnologia odierna non è quella che si utilizzava quando è stata concepita e adottata la direttiva 95/46/CE. Fenomeni tecnologici quali il cloud computing, la pubblicità comportamentale, le reti sociali, il telepedaggio e i dispositivi di localizzazione geografica hanno modificato profondamente il modo in cui vengono trattati i dati personali e costituiscono sfide enormi per la protezione dei dati. Una revisione delle norme europee di protezione dei dati dovrà affrontare efficacemente queste problematiche.

15. Il secondo fattore è la globalizzazione. Grazie alla progressiva eliminazione degli ostacoli agli scambi, le imprese hanno acquisito una crescente dimensione globale. Il trattamento transfrontaliero dei dati e i trasferimenti internazionali sono aumentati in maniera esponenziale negli ultimi anni. Inoltre, grazie alle tecnologie dell'informazione e della comunicazione, il trattamento dei dati ha raggiunto una diffusione capillare: Internet e il cloud computing hanno permesso di delocalizzare il trattamento di grandi quantità di dati su scala mondiale. Nell'ultimo decennio si è altresì assistito a un incremento delle attività giudiziarie e di polizia svolte a livello internazionale per contrastare il

([6]) In particolare (cfr. il punto 77 del parere): nessuna esigenza di modificare i principi esistenti, ma una chiara necessità di altre disposizioni amministrative; il vasto campo di applicazione della legislazione sulla protezione dei dati applicabile a tutti gli usi dei dati personali non dovrebbe cambiare; la legislazione sulla protezione dei dati dovrebbe permettere un approccio equilibrato nei casi concreti e inoltre dovrebbe consentire alle autorità per la protezione dei dati di fissare delle priorità; il sistema dovrebbe applicarsi interamente all'utilizzo dei dati personali ai fini dell'applicazione della legge, sebbene ulteriori misure appropriate possano rendersi necessarie per trattare problemi speciali in questo settore.

([7]) Documento WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Il suo messaggio principale è che una modifica legislativa costituisce una buona occasione per chiarire alcune norme e principi fondamentali (ad esempio consenso, trasparenza), introdurre alcuni principi nuovi (quali i concetti di «privacy by design» (tutela della vita privata fin dalla progettazione) e il principio di responsabilità), rafforzare l'efficacia attraverso la modernizzazione normativa (ad esempio limitando i requisiti di notifica esistenti) e integrarli tutti in un quadro giuridico globale (compresa la cooperazione di polizia e giudiziaria).

([8]) I punti menzionati nella conferenza stampa sono disponibili sul sito Internet del GEPD al seguente indirizzo: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

terrorismo e altre forme di criminalità organizzata internazionale, sostenute da un enorme scambio di informazioni a fini di contrasto. Per tutti questi motivi è necessario valutare attentamente il modo di garantire un'efficace protezione dei dati personali nel mondo globalizzato senza ostacolare in maniera considerevole le attività internazionali di trattamento dei dati.

16. Il terzo fattore è il trattato di Lisbona. L'entrata in vigore del trattato di Lisbona segna una nuova era per la protezione dei dati. L'articolo 16 del TFUE non solo contiene un diritto individuale dell'interessato, ma fornisce anche una base giuridica diretta per una solida normativa in materia di protezione dei dati valida in tutta l'UE. Inoltre, la soppressione della struttura a pilastri sancisce l'obbligo per il Parlamento europeo e il Consiglio di garantire la protezione dei dati in tutti i settori del diritto dell'UE. In altri termini, consente l'emanazione di un quadro giuridico globale per la protezione dei dati applicabile al settore privato, al settore pubblico negli Stati membri e alle istituzioni e agli organismi dell'UE. A tale proposito il programma di Stoccolma ([9]) afferma coerentemente che l'Unione deve garantire una strategia globale in materia di protezione dei dati all'interno dell'UE e nell'ambito delle relazioni con i paesi terzi.

17. Il quarto fattore è rappresentato dagli sviluppi paralleli che stanno avendo luogo nell'ambito delle organizzazioni internazionali. Sono in corso vari dibattiti sulla modernizzazione degli strumenti giuridici esistenti per la protezione dei dati. A tale proposito è importante citare le attuali riflessioni intraprese in merito alla futura revisione della Convenzione 108 del Consiglio d'Europa ([10]) e delle linee guida dell'OCSE sulla protezione della vita privata ([11]). Un altro sviluppo importante riguarda l'adozione di norme internazionali sulla protezione dei dati personali e della vita privata, da cui potrebbe eventualmente scaturire l'adozione di uno strumento globale vincolante sulla protezione dei dati. Tutte queste iniziative meritano pieno sostegno. Il loro obiettivo comune deve essere garantire una protezione efficace e omogenea in un ambiente ad alto contenuto tecnologico e globalizzato.

3. **Principali prospettive**

3.1. *La protezione dei dati promuove la fiducia e deve sostenere altri interessi (pubblici)*

18. Un solido quadro di protezione dei dati è la conseguenza necessaria dell'importanza attribuita alla protezione dei dati nell'ambito del trattato di Lisbona, in particolare dall'articolo 8 della Carta dei diritti fondamentali dell'Unione e dall'articolo 16 del TFUE, nonché dello stretto collegamento con l'articolo 7 della Carta ([12]).

19. Un solido quadro di protezione dei dati, tuttavia, è anche al servizio di interessi pubblici e privati più ampi in una società dell'informazione caratterizzata da un trattamento dei dati pervasivo. La protezione dei dati promuove la fiducia, e la fiducia è una componente essenziale per il buon funzionamento della nostra società. È indispensabile che le misure di protezione dei dati siano concepite in maniera tale che — per quanto possibile — possano sostenere attivamente anziché ostacolare altri diritti e interessi legittimi.

20. Esempi importanti di altri interessi legittimi sono un'economia europea forte, la sicurezza delle persone e la responsabilità dei governi.

21. Lo sviluppo economico dell'UE va di pari passo con l'introduzione e la commercializzazione di nuovi servizi e tecnologie. Nella società dell'informazione la comparsa e il buon esito della diffusione dei servizi e delle tecnologie dell'informazione e della comunicazione (TIC) dipendono dalla fiducia. Se le persone non hanno fiducia nelle TIC, queste tecnologie potrebbero fallire ([13]). E le persone avranno fiducia nelle TIC solo se i loro dati saranno protetti efficacemente. La protezione dei dati, pertanto, deve essere parte integrante di tecnologie e servizi. Un solido quadro di protezione dei dati favorisce l'economia europea, purché tale quadro sia non solo solido ma anche concepito in maniera adeguata. In quest'ottica una maggiore armonizzazione nell'UE e la riduzione al minimo degli oneri amministrativi rivestono un'importanza fondamentale (cfr. il capo 5 del presente parere).

22. Negli ultimi anni si è parlato molto della necessità di raggiungere un equilibrio tra vita privata e sicurezza, specialmente riguardo agli strumenti di trattamento e scambio dei dati nel settore della cooperazione di polizia e giudiziaria ([14]). La protezione dei dati è stata piuttosto spesso erroneamente ritenuta un ostacolo alla piena protezione della sicurezza fisica delle persone ([15]) o per lo meno una condizione inevitabile da rispettare da parte delle autorità di contrasto. Si tratta tuttavia di una visione riduttiva. Un solido quadro di protezione dei dati può affinare e rafforzare la sicurezza. In base ai principi di protezione dei dati — se correttamente applicati — i responsabili del trattamento sono tenuti a garantire che le informazioni siano precise e aggiornate e che i dati personali superflui che non sono necessari ai fini delle attività di contrasto siano eliminati dai sistemi. Si può analogamente segnalare l'obbligo di attuare le misure tecnologiche e organizzative volte a garantire la sicurezza dei

([9]) Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini, (GU C 115 del 4.5.2010, pag. 1), a pag. 10.

([10]) Convenzione 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STE n. 108 del 28 gennaio 1981.

([11]) Linee guida dell'OCSE sulla protezione della vita privata e dei flussi transfrontalieri di dati personali, pubblicate su http://www.oecd.org

([12]) L'importanza della protezione dei dati e il collegamento con la vita privata sancito nella Carta sono stati sottolineati dalla Corte di giustizia nella sentenza del 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Schecke*, non ancora pubblicata nella Raccolta.

([13]) Cfr. il parere del GEPD del 18 marzo 2010 sulla promozione della fiducia nella società dell'informazione tramite l'incentivazione della protezione dei dati e della vita privata, (GU C 280 del 16.10.2010, pag. 1), punto 113.

([14]) Cfr. ad esempio il parere del GEPD del 10 luglio 2009 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini», (GU C 276 del 17.9.2009, pag. 8).

([15]) Il concetto di sicurezza è più ampio di quello di sicurezza fisica, ma, al fine di illustrare gli argomenti esaminati, nel presente contesto viene utilizzato nel suo significato più limitato.

sistemi, quali le disposizioni finalizzate a proteggerli dalla divulgazione o dall'accesso non autorizzati, come quelle sviluppate nel settore della protezione dei dati.

23. L'osservanza dei principi di protezione dei dati può ulteriormente garantire che le autorità di contrasto agiscano nel rispetto dello stato di diritto che stimola la fiducia nel loro operato e promuove pertanto in senso più ampio la fiducia nelle nostre società. La giurisprudenza elaborata a norma dell'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo garantisce alle autorità giudiziarie e di polizia la possibilità di trattare tutti i dati pertinenti per il loro lavoro, ma non in maniera illimitata. La protezione dei dati richiede pesi e contrappesi (per quanto riguarda la polizia e la giustizia, cfr. il capo 9 del parere).

24. Nelle società democratiche i governi sono responsabili di tutte le loro attività, anche dell'uso dei dati personali per la soddisfazione dei vari interessi pubblici di cui sono al servizio, il che va dalla pubblicazione dei dati su Internet per motivi di trasparenza all'utilizzo dei dati a sostegno di politiche in settori quali la salute pubblica, i trasporti, la fiscalità e la sorveglianza delle persone a fini di contrasto. Un solido quadro di protezione dei dati permette ai governi di rispettare gli obblighi loro incombenti e di rendere conto del proprio operato, nell'ambito del buon governo.

3.2. *Conseguenze per il quadro giuridico sulla protezione dei dati*

3.2.1. Necessità di una maggiore armonizzazione

25. La comunicazione ha giustamente individuato che una delle lacune fondamentali del quadro attuale è che lascia agli Stati membri un eccessivo margine di discrezione nella trasposizione delle disposizioni europee nell'ordinamento nazionale. La mancanza di armonizzazione ha molte conseguenze negative in una società dell'informazione in cui le frontiere fisiche tra gli Stati membri diventano sempre meno rilevanti (cfr. il capo 5 del parere).

3.2.2. I principi generali di protezione dei dati sono tuttora validi

26. Un primo e più formale motivo per cui i principi generali di protezione dei dati non devono e non possono essere modificati è di natura giuridica. Tali principi sono fissati dalla Convenzione 108 del Consiglio d'Europa, che è vincolante per tutti gli Stati membri. Questa convenzione è la base della protezione dei dati nell'UE. Alcuni dei principi fondamentali, inoltre, sono espressamente indicati nell'articolo 8 della Carta dei diritti fondamentali dell'Unione. Per modificare tali principi, pertanto, occorrerebbe modificare i trattati.

27. Questo motivo, tuttavia, non è l'unico. Esistono anche altre ragioni sostanziali per non modificare i principi generali. Il GEPD è fermamente convinto che una società dell'informazione non possa e non debba funzionare senza un'adeguata protezione della vita privata e dei dati personali. Quando il numero delle informazioni trattate aumenta, occorre anche migliorare la protezione. Una società dell'informazione in cui vengono trattate considerevoli quantità di dati su chiunque deve fondarsi sul concetto di controllo da parte dell'individuo, in modo da permettere al soggetto interessato di agire come persona e di esercitare le proprie libertà, quali le libertà di espressione e di parola, in una società democratica.

28. Inoltre, è difficile immaginare il controllo dell'individuo senza prevedere l'obbligo, per i responsabili del trattamento dei dati, di limitare tale attività conformemente ai principi di necessità, proporzionalità e limitazione delle finalità. È altrettanto difficile immaginare il controllo da parte dell'individuo senza il riconoscimento di diritti degli interessati quali i diritti di accesso, rettifica e cancellazione o blocco dei dati.

3.2.3. Prospettiva dei diritti fondamentali

29. Il GEPD sottolinea che la protezione dei dati é riconosciuta quale diritto fondamentale. Questo non significa che la protezione dei dati deve sempre *prevalere* su altri diritti e interessi importanti in una società democratica, ma ha conseguenze per la natura e la portata della protezione che deve essere fornita nell'ambito di un quadro giuridico dell'UE, al fine di garantire che i requisiti in materia di protezione dei dati vengano sempre presi *adeguatamente* in considerazione.

30. Queste conseguenze principali possono essere definite come segue:

— la protezione deve essere efficace. Un quadro giuridico deve prevedere strumenti che permettano alle persone di esercitare i propri diritti nella pratica,

— il quadro deve rimanere stabile nel lungo periodo,

— la protezione deve essere garantita in qualsiasi circostanza e non dipendere dalle preferenze politiche di un determinato periodo,

— limitazioni all'esercizio del diritto potrebbero rendersi necessarie. Queste, tuttavia, dovranno tuttavia essere eccezionali, debitamente giustificate e non incidere mai sugli elementi essenziali del diritto stesso ([16]).

Il GEPD raccomanda alla Commissione di tenere conto di queste conseguenze nel proporre soluzioni legislative.

3.2.4. Necessità di nuove misure legislative

31. La comunicazione si concentra giustamente sulla necessità di rafforzare le misure legislative in materia di protezione dei dati. A tale proposito è opportuno ricordare che nel documento del Gruppo di lavoro sul futuro della privacy ([17]) le autorità di protezione dei dati avevano sottolineato la necessità di rafforzare il ruolo svolto dai

([16]) Cfr. anche il parere del GEPD del 25 luglio 2007 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati, punto 17, che si basa sulla giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia.

([17]) Cfr. nota 7.

differenti attori nel settore della protezione dei dati, in particolare dalle persone interessate, dai responsabili del trattamento e dalle autorità di controllo stesse.

32. Sembra che le parti interessate concordino ampiamente sulla necessità di rafforzare il quadro legislativo — tenendo conto degli sviluppi tecnologici e della globalizzazione — per garantire una protezione dei dati ambiziosa ed efficace anche in futuro. Come già indicato al punto 7, sono questi i criteri sulla cui base il GEPD valuta tutte le soluzioni proposte.

3.2.5. Completezza quale *conditio sine qua non*

33. Come viene ricordato nella comunicazione, la direttiva 95/46/CE si applica a tutte le attività di trattamento dei dati personali negli Stati membri, sia nel settore pubblico che in quello privato, ad eccezione delle attività che non rientrano nel campo di applicazione del precedente diritto comunitario ([18]). Benché fosse prevista dall'ex trattato, dopo l'entrata in vigore del trattato di Lisbona questa eccezione non è più necessaria. L'eccezione contravviene peraltro il testo e in ogni caso lo spirito dell'articolo 16 del TFUE.

34. Il GEPD ritiene che uno strumento giuridico globale per la protezione dei dati che contempli la cooperazione di polizia e giudiziaria in materia penale debba essere considerato come uno dei principali miglioramenti che un nuovo quadro giuridico possa apportare. È una *conditio sine qua non* per garantire un'efficace protezione dei dati in futuro.

35. Il GEPD illustra le seguenti argomentazioni a sostegno di tale affermazione:

— la distinzione tra le attività di trattamento dei dati svolte nel settore privato e a fini di contrasto non è netta. Gli organismi del settore privato possono trattare dati che in ultima analisi vengono utilizzati a fini di contrasto (esempio: i dati PNR ([19])), mentre in altri casi sono tenuti a conservare i dati sempre a fini di contrasto (esempio: la direttiva sulla conservazione dei dati ([20])),

— non esistono differenze fondamentali tra le autorità giudiziarie e di polizia e altre autorità di contrasto (fiscali, doganali, antifrode e competenti per l'immigrazione) soggette alla direttiva 95/46/CE,

— come accuratamente illustrato nella comunicazione, lo strumento giuridico per la protezione dei dati attualmente applicabile alle autorità giudiziarie e di polizia (la decisione quadro 2008/977/GAI ([21])) è inadeguato,

— la maggior parte degli Stati membri ha recepito la direttiva 95/46/CE e la Convenzione 108 nel proprio ordinamento nazionale, rendendole applicabili anche alle autorità giudiziarie e di polizia nazionali.

36. L'inclusione della polizia e della giustizia nello strumento giuridico generale non solo offrirebbe maggiori garanzie ai cittadini, ma agevolerebbe anche il compito delle autorità di polizia. La necessità di applicare regolamentazioni diverse comporta procedure gravose e inutilmente lunghe e ostacola la cooperazione internazionale (cfr. di seguito il capo 9 del parere). Ne consegue altresì l'opportunità di includere nello strumento le attività di trattamento svolte dai servizi di sicurezza nazionali, nella misura in cui questo sia possibile allo stato attuale del diritto dell'Unione europea.

3.2.6. Neutralità tecnologica

37. Il periodo trascorso dall'adozione della direttiva 95/46/CE nel 1995 può essere definito tumultuoso dal punto di vista tecnologico. Vengono introdotti di frequente nuovi sviluppi e dispositivi tecnologici, che in molti casi hanno modificato profondamente le modalità di trattamento dei dati personali. La società dell'informazione non può più essere considerata un ambiente parallelo al quale le persone possono partecipare su base volontaria, ma è divenuta parte integrante della nostra vita quotidiana. Solo a titolo di esempio, il concetto di un internet degli oggetti ([22]) istituisce interconnessioni tra gli oggetti fisici e le informazioni online ad essi correlate.

38. La tecnologia continuerà a svilupparsi, con le conseguenze che ne deriveranno per il nuovo quadro giuridico, che dovrà essere efficace per un maggior numero di anni e al tempo stesso non ostacolare ulteriori sviluppi tecnologici. È pertanto necessario che le disposizioni giuridiche siano tecnologicamente neutre. Il quadro deve tuttavia garantire anche una maggiore certezza del diritto per le imprese e per le persone, che devono capire ciò che ci si aspetta da loro e poter esercitare i propri diritti. È pertanto necessario che le disposizioni giuridiche siano precise.

39. Il GEPD ritiene che uno strumento giuridico generale per la protezione dei dati debba essere formulato, per quanto possibile, in maniera tecnologicamente neutra. Ne consegue la necessità di formulare i diritti e gli obblighi dei vari attori in maniera generale e neutra in modo da garantirne, in linea di principio, la validità e l'applicabilità indipendentemente dalla tecnologia scelta per il trattamento dei dati personali. Non esistono alternative, considerata la rapidità con cui si susseguono i progressi tecnologici al giorno d'oggi. Il GEPD suggerisce di introdurre, accanto

([18]) Il presente parere si concentrerà principalmente sull'ex terzo pilastro (cooperazione di polizia e giudiziaria in materia penale), poiché l'ex secondo pilastro non è solo un settore più complesso del diritto UE (come peraltro riconosciuto dall'articolo 16 del TFUE e dall'articolo 39 UE), ma è anche meno pertinente per il trattamento dei dati.

([19]) Cfr. ad esempio la comunicazione della Commissione sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi, COM(2010) 492 definitivo.

([20]) Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU L 105 del 13.4.2006, pag. 54).

([21]) Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU L 350 del 30.12.2008, pag. 60).

([22]) Quale definito nella comunicazione «L'internet degli oggetti — Un piano d'azione per l'Europa», COM(2009) 278 definitivo.

ai principi di protezione dei dati esistenti, nuovi diritti «tecnologicamente neutri» che potrebbero avere un'importanza specifica nell'ambiente elettronico in rapida evoluzione (cfr. principalmente i capi 6 e 7).

3.2.7. Lungo periodo: certezza del diritto più a lungo termine

40. La direttiva 95/46/CE è, da quindici anni a questa parte, l'atto centrale della legislazione sulla protezione dei dati nell'UE. È stata recepita negli ordinamenti degli Stati membri e applicata dai differenti attori. Nell'arco degli anni la sua applicazione ha beneficiato delle esperienze pratiche e degli ulteriori orientamenti forniti dalla Commissione, dalle autorità di protezione dei dati (a livello nazionale e nell'ambito del Gruppo di lavoro articolo 29) nonché dagli organi giudiziari nazionali ed europei.

41. È opportuno sottolineare che questi sviluppi richiedono tempo e che — proprio perché si tratta di un quadro generale che dà attuazione a un diritto fondamentale — questo tempo è necessario per creare certezza del diritto e stabilità. Deve essere elaborato un nuovo strumento giuridico generale con l'ambizione di essere in grado di creare certezza del diritto e stabilità più a lungo termine, ricordando che è molto difficile prevedere il modo in cui la tecnologia e la globablizzazione si svilupperanno ulteriormente. In ogni caso, il GEPD sostiene appieno l'obiettivo di creare certezza del diritto più a lungo termine rispetto alla prospettiva della direttiva 95/46/CE. In sintesi, se la tecnologia si sviluppa a un ritmo sostenuto, occorre garantire la stabilità del diritto.

3.2.8. Breve periodo: utilizzare meglio gli strumenti esistenti

42. Nel breve periodo è essenziale garantire l'efficacia delle misure legislative esistenti, concentrandosi in primo luogo sulla loro applicazione, a livello sia nazionale che dell'UE (cfr. il capo 11 del presente parere).

B. ELEMENTI DI UN NUOVO QUADRO

4. Approccio globale

43. Il GEPD condivide appieno l'approccio globale alla protezione dei dati che non è solo il titolo, ma anche il punto di partenza della comunicazione e prevede necessariamente l'estensione dell'applicazione delle norme generali di protezione dei dati alla cooperazione di polizia e giudiziaria in materia penale ([23]).

44. Tuttavia, il GEPD rileva altresì che la Commissione non intende includere tutte le attività di trattamento dei dati in questo strumento giuridico generale. In particolare, sarà escluso il trattamento dei dati da parte di istituzioni, organi, organismi e agenzie dell'Unione. La Commissione si limita ad affermare che «valuterà se occorra adeguare altri atti legislativi al nuovo quadro giuridico generale».

([23]) Cfr. la pagina 14 della comunicazione e la sezione 3.2.5 del presente parere.

45. Il GEPD è nettamente favorevole all'inclusione del trattamento dei dati a livello dell'UE nel quadro giuridico generale. Ricorda che questa era l'intenzione originale dell'ex articolo 286 CE, che menzionava per la prima volta la protezione dei dati a livello del trattato. L'articolo 286 CE affermava semplicemente che gli strumenti giuridici con riguardo al trattamento dei dati personali si applicano anche alle istituzioni. Soprattutto, un testo giuridico evita il rischio di discrepanze tra disposizioni e risulterebbe più adeguato per lo scambio di dati tra il livello dell'UE e gli organismi del settore pubblico e privato degli Stati membri. Scongiurerebbe altresì il rischio che, in seguito alla modifica della direttiva 95/46/CE, venga meno l'interesse politico di modificare il regolamento (CE) n. 45/2001 o di accordare sufficiente priorità a tale modifica al fine di evitare discrepanze nelle date di entrata in vigore.

46. Il GEPD esorta la Commissione — nel caso in cui stabilisca l'impossibilità di includere il trattamento dei dati a livello dell'UE nello strumento giuridico generale — a impegnarsi a proporre un adeguamento del regolamento (CE) n. 45/2001 (non a «valutare se occorra» procedere in tal senso) nel più breve tempo possibile e preferibilmente entro la fine del 2011.

47. È altrettanto importante che la Commissione garantisca che non vengano trascurati altri settori, in particolare:

— la protezione dei dati nel settore della politica estera e di sicurezza comune sulla base dell'articolo 39 del TUE ([24]);

— regimi settoriali di protezione dei dati per organismi UE quali Europol, Eurojust e per sistemi d'informazione su vasta scala, nella misura in cui sussista la necessità di adeguarli al nuovo strumento giuridico;

— la direttiva e-Privacy 2002/58/CE, nella misura in cui sussista la necessità di adeguarla al nuovo strumento giuridico.

48. Infine, uno strumento giuridico generale per la protezione dei dati può e probabilmente deve essere integrato da specifici regolamenti settoriali supplementari, che disciplinino ad esempio la cooperazione giudiziaria e di polizia, ma anche altri settori ([25]). Laddove necessario e conformemente al principio di sussidiarietà, tali regolamenti supplementari dovrebbero essere adottati a livello dell'UE. Gli Stati membri possono definire norme supplementari in settori specifici ove ciò sia giustificato (cfr. la sezione 5.2).

([24]) Cfr. anche il parere del GEPD del 24 novembre 2010 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio — «La politica antiterrorismo dell'UE: principali risultati e sfide future», punto 31.

([25]) Cfr. anche il documento del Gruppo di lavoro sul futuro della privacy (nota a piè di pagina 7), punti 18-21.

5. **Maggiore armonizzazione e semplificazione**

5.1. *La necessità di armonizzazione*

49. L'armonizzazione riveste un'enorme importanza per la normativa UE sulla protezione dei dati. La comunicazione ha correttamente sottolineato che la protezione dei dati ha una dimensione «mercato interno» che si esplica nella necessità di assicurare la libera circolazione dei dati personali tra gli Stati membri nel mercato interno. Ciononostante, il livello di armonizzazione derivante dalla direttiva attuale è stato ritenuto tutt'altro che soddisfacente. La comunicazione riconosce che questa è una delle preoccupazioni più frequenti delle parti interessate. In particolare, le parti interessate sottolineano la necessità di migliorare la certezza giuridica, ridurre gli oneri amministrativi e assicurare condizioni eque agli operatori economici. Come giustamente osserva la Commissione, particolarmente problematica è la situazione dei responsabili del trattamento stabiliti in più Stati membri, di cui devono rispettare le disposizioni delle legislazioni nazionali vigenti (ed eventualmente divergenti) in materia di protezione dei dati ([26]).

50. L'armonizzazione non è importante solo per il mercato interno, ma anche al fine di garantire un'adeguata protezione dei dati. L'articolo 16 del TFUE stabilisce che «ogni persona» ha diritto alla protezione dei dati di carattere personale che la riguardano. Affinché questo diritto venga effettivamente rispettato, occorre garantire un livello di protezione dei dati equivalente in tutta l'UE. Il documento del Gruppo di lavoro sul futuro della privacy ha evidenziato che numerose misure relative alle posizioni degli interessati non sono state attuate o interpretate uniformemente in tutti gli Stati membri ([27]). In un mondo globalizzato e interconnesso, queste divergenze potrebbero pregiudicare o limitare la protezione delle persone.

51. Il GEPD ritiene che una maggiore e migliore armonizzazione sia uno dei principali obiettivi del processo di revisione. Il GEPD accoglie con favore l'impegno della Commissione a esaminare i mezzi per conseguire una maggiore armonizzazione delle norme di protezione dei dati a livello dell'UE. Ciononostante, rileva con una certa sorpresa che in questa fase la comunicazione non propone alcuna opzione concreta. Pertanto, provvede egli stesso a indicare alcuni settori in cui una maggiore convergenza è particolarmente urgente (cfr. la sezione 5.3). Per conseguire una maggiore armonizzazione in questi settori occorre non solo ridurre il margine di manovra nella trasposizione della normativa a livello nazionale, ma anche impedire la non corretta attuazione da parte degli Stati membri (cfr. anche il capo 11) e garantire un'applicazione più coerente e coordinata (cfr. anche il capo 10).

([26]) Cfr. la pagina 10 della comunicazione.

([27]) Cfr. il documento del Gruppo di lavoro sul futuro della privacy (nota a piè di pagina 7), punto 70. Il documento si riferisce in particolare alle disposizioni in materia di responsabilità e alla possibilità di presentare una domanda di risarcimento dei danni non materiali.

5.2. *Ridurre il margine di manovra nell'attuazione della direttiva*

52. La direttiva contiene una serie di disposizioni formulate in maniera vaga e che di conseguenza lasciano un margine considerevole per un'applicazione divergente. Il considerando 9 della direttiva conferma espressamente che gli Stati membri dispongono di un certo margine di manovra e che, entro tale margine di manovra, potranno verificarsi divergenze nell'applicazione. Numerose disposizioni sono state attuate in maniera diversa dagli Stati membri, tra cui alcune di importanza fondamentale ([28]). Questa situazione non è soddisfacente e occorre conseguire una maggiore convergenza.

53. Questo non significa che la diversità debba essere esclusa a priori. In determinati settori la flessibilità potrebbe essere necessaria al fine di preservare specificità giustificate, interessi pubblici importanti o l'autonomia istituzionale degli Stati membri. Il GEPD ritiene che il margine di divergenza tra gli Stati membri debba essere limitato in particolare alle seguenti situazioni specifiche:

— libertà d'espressione: nell'ambito del quadro attuale (articolo 9), gli Stati membri possono prevedere esenzioni e deroghe per il trattamento di dati personali effettuato a scopi giornalistici o di espressione artistica o letteraria. Tale flessibilità sembra giustificata, ovviamente fatti salvi i limiti previsti dalla Carta e dalla CEDU, in considerazione delle diverse tradizioni e delle differenze culturali che possono esistere in questo settore nei vari Stati membri. Ciò non rappresenterebbe tuttavia un ostacolo a un eventuale aggiornamento dell'attuale articolo 9 alla luce degli sviluppi relativi a Internet,

— specifici interessi pubblici: nell'ambito del quadro attuale (articolo 13), gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti qualora tale restrizione costituisca una misura necessaria alla salvaguardia di un interesse pubblico importante quale la sicurezza dello Stato, la difesa, la pubblica sicurezza, eccetera. Questa competenza degli Stati membri resta giustificata. Laddove possibile, tuttavia, occorre armonizzare maggiormente l'interpretazione delle deroghe (cfr. la sezione 9.1). L'attuale portata della deroga all'articolo 6, paragrafo 1, inoltre, appare eccessivamente ampia,

— mezzi di ricorso, sanzioni e procedure amministrative: un quadro europeo deve precisare le condizioni principali, ma allo stato attuale del diritto dell'Unione la definizione di sanzioni, mezzi di ricorso, norme procedurali e modalità di ispezioni applicabili a livello nazionale deve restare di competenza degli Stati membri.

([28]) Esistono alcuni approcci divergenti anche per quanto riguarda i dati manuali.

5.3. *Settori che richiedono una maggiore armonizzazione*

54. *Definizioni* (articolo 2 della direttiva 95/46/CE). Le definizioni sono la base del sistema giuridico e devono essere interpretate uniformemente in tutti gli Stati membri, senza margini applicativi. Nell'ambito del quadro attuale sono sorte divergenze, ad esempio per quanto riguarda il concetto di responsabile del trattamento ([29]). Al fine di assicurare una maggiore certezza del diritto il GEPD suggerisce di aggiungere ulteriori elementi all'elenco attualmente contemplato dall'articolo 2, quali dati anonimi, dati pseudonimi, dati giudiziari, trasferimento di dati e incaricato della protezione dei dati.

55. *Liceità dei trattamenti (articolo 5).* Il nuovo strumento giuridico deve essere quanto più preciso possibile per quanto riguarda gli elementi essenziali che determinano la liceità dei trattamenti di dati. L'articolo 5 della direttiva (nonché il suo considerando 9), che impone agli Stati membri di precisare le condizioni alle quali i trattamenti di dati personali sono leciti, potrebbe pertanto non essere più necessario in un quadro futuro.

56. *Motivi che legittimano il trattamento dei dati* (articoli 7 e 8). La definizione delle basi giuridiche del trattamento dei dati è un elemento essenziale di qualsiasi normativa in materia di protezione dei dati. Gli Stati membri non devono poter introdurre motivi aggiuntivi o modificati che legittimano il trattamento dei dati né escluderne alcuno. La possibilità di deroghe deve essere esclusa o limitata (particolarmente per quanto riguarda i dati sensibili ([30])). In un nuovo strumento giuridico occorre formulare chiaramente i motivi che legittimano il trattamento dei dati, riducendo così il margine discrezionale a livello di recepimento e applicazione. In particolare, potrebbe essere necessario specificare ulteriormente il concetto di consenso (cfr. la sezione 6.5). Inoltre, il motivo basato sull'interesse legittimo del responsabile del trattamento [articolo 7, lettera (f)] dà adito, a causa della sua flessibilità, a interpretazioni ampiamente divergenti. Occorre precisarlo meglio. Un'altra disposizione che probabilmente dovrà essere specificata è l'articolo 8, paragrafo 2, lettera b), che consente il trattamento dei dati sensibili qualora sia necessario per assolvere gli obblighi e i diritti specifici del responsabile del trattamento in materia di diritto del lavoro ([31]).

57. *Diritti delle persone interessate* (articoli 10-15). Questo è uno dei settori in cui non tutti gli elementi della direttiva sono stati attuati e interpretati coerentemente dagli Stati membri. I diritti delle persone interessate sono un elemento centrale per un'efficace protezione dei dati. Di conseguenza, occorre ridurre considerevolmente il margine di manovra. Il GEPD raccomanda di garantire in tutta l'UE l'uniformità delle informazioni fornite alle persone interessate dal responsabile del trattamento.

58. *Trasferimenti internazionali* (articoli 25-26). Questo è un settore che ha sollevato vaste critiche per la mancanza di una prassi uniforme nell'UE. Le parti interessate hanno criticato la grande disparità di interpretazione e attuazione delle decisioni della Commissione sull'adeguatezza da parte degli Stati membri. Le «norme vincolanti d'impresa» (Binding Corporate Rules — BCR) sono un ulteriore aspetto su cui il GEPD raccomanda una maggiore armonizzazione (cfr. il capo 9).

59. *Autorità nazionali di protezione dei dati* (articolo 28). Le autorità nazionali di protezione dei dati sono soggette a norme ampiamente divergenti nei 27 Stati membri, in particolare per quanto riguarda lo status, le risorse e i poteri loro conferiti. L'articolo 28 ha in parte contribuito a tale divergenza per la sua mancanza di precisione ([32]) e deve essere specificato ulteriormente, in conformità della sentenza della Corte di giustizia dell'Unione europea nella causa C-518/07 ([33]) (cfr. di seguito il capo 10).

5.4. *Semplificazione del sistema di notificazione*

60. Gli obblighi in materia di notificazione (articoli 18-21 della direttiva 95/46/CE) sono un altro settore in cui finora è stata concessa una notevole libertà agli Stati membri. La comunicazione riconosce giustamente che un sistema armonizzato ridurrebbe i costi e gli oneri amministrativi a carico dei responsabili del trattamento ([34]).

61. Questo è un settore in cui la semplificazione deve essere l'obiettivo principale. La revisione del quadro di protezione dei dati costituisce un'occasione unica per semplificare e/o ridurre ulteriormente l'ambito di applicazione degli obblighi attuali in materia di notificazione. La comunicazione riconosce che i responsabili del trattamento concordano in generale che l'attuale sistema di notificazione è alquanto gravoso e di per sé non aggiunge molto alla protezione dei dati personali ([35]). Il GEPD accoglie pertanto con favore l'impegno della Commissione a esaminare diversi modi per semplificare l'attuale sistema di notificazione.

62. Il GEPD ritiene che il punto di partenza di tale semplificazione debba essere il passaggio da un sistema il cui la notificazione è la norma, salvo disposizione contraria (ad esempio un «sistema di deroghe»), a un sistema più mirato. Il sistema di deroghe si è rivelato inefficiente poiché è stato attuato in maniera disomogenea nei vari Stati membri ([36]). Il GEPD suggerisce di valutare le seguenti alternative:

([29]) Cfr. il parere 1/2010 del Gruppo di lavoro articolo 29 sui concetti di «responsabile del trattamento» e «incaricato del trattamento» (WP 169).

([30]) L'articolo 8, paragrafi 4 e 5, in talune circostanze autorizza attualmente gli Stati membri a prevedere ulteriori deroghe per quanto riguarda i dati sensibili.

([31]) Cfr., a tale proposito, la prima relazione della Commissione sull'applicazione della direttiva sulla protezione dei dati, menzionata in precedenza, pag. 14.

([32]) Documento del Gruppo di lavoro sul futuro della privacy, punto 87.

([33]) Causa C-518/07, *Commissione contro Germania*, non ancora pubblicata nella Raccolta.

([34]) Cfr. nota 26.

([35]) Cfr. nota 26.

([36]) Relazione del Gruppo di lavoro articolo 29 sull'obbligo di notifica alle autorità di controllo nazionali, sul miglior utilizzo di deroghe e semplificazioni e sul ruolo degli incaricati della protezione dei dati nell'Unione europea, WP 106, 2005, pag. 7.

— limitare l'obbligo di notificazione a specifiche tipologie di trattamento dei dati che comportano rischi specifici (da tali notifiche potrebbero scaturire ulteriori iniziative quali il controllo preventivo del trattamento);

— un semplice obbligo di registrazione che preveda la registrazione da parte dei responsabili del trattamento (anziché la registrazione dettagliata di tutte le operazioni di trattamento dei dati).

Inoltre potrebbe essere introdotto un modulo di notifica uniforme per tutta l'UE che permetta di garantire approcci armonizzati in merito alle informazioni richieste.

63. La revisione del sistema di notificazione attuale non deve pregiudicare il miglioramento degli obblighi di controllo preventivo per determinate operazioni di trattamento che é probabile presentino rischi specifici (quali i sistemi d'informazione su vasta scala). Il GEPD è favorevole a includere nel nuovo strumento giuridico un elenco non esaustivo dei casi in cui è necessario tale controllo preventivo. Il regolamento (CE) n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE costituisce un utile modello in tal senso ([37]).

5.5. *Un regolamento, non una direttiva*

64. Infine, il GEPD ritiene che il processo di revisione rappresenti altresì un'occasione per riesaminare il tipo di strumento giuridico più indicato per la protezione dei dati. Un regolamento, uno strumento unico che sia direttamente applicabile negli Stati membri, è il mezzo più efficace per proteggere il diritto fondamentale alla protezione dei dati e creare un vero mercato interno in cui i dati personali possano circolare liberamente e in cui venga assicurato lo stesso livello di protezione indipendentemente dal paese o dal settore in cui i dati vengono trattati.

65. Un regolamento ridurrebbe lo spazio esistente per interpretazioni contraddittorie e di differenze ingiustificate nel recepimento e nell'applicazione della normativa. Ridurrebbe altresì l'importanza di individuare il diritto applicabile alle operazioni di trattamento nell'UE, che è uno degli aspetti più controversi del sistema attuale (cfr. il capo 9).

66. Nel settore della protezione dei dati un regolamento è tanto più giustificato poiché

— l'articolo 16 del TFUE ha innalzato il diritto alla protezione dei dati personali al livello del trattato e prevede — o addirittura impone — un livello di protezione uniforme delle persone nell'UE;

— il trattamento dei dati avviene in un ambiente elettronico in cui le frontiere interne tra gli Stati membri sono divenute meno rilevanti.

67. La scelta di un regolamento quale strumento generale ammette, se del caso, disposizioni destinate direttamente agli Stati membri qualora sia necessaria la flessibilità. Inoltre non influisce sulla competenza, da parte degli Stati membri, di adottare, se del caso, norme aggiuntive per la protezione dei dati, conformemente al diritto dell'UE.

6. **Rafforzare i diritti delle persone**

6.1. *Necessità di rafforzare i diritti*

68. Il GEPD è assolutamente favorevole alla proposta di rafforzare i diritti delle persone avanzata nella comunicazione; gli strumenti giuridici esistenti, infatti, non garantiscono appieno l'effettiva protezione che è necessaria in un mondo digitalizzato sempre più complesso.

69. Da un lato, lo sviluppo di un mondo digitalizzato comporta un brusco incremento in termini di raccolta, utilizzo e ulteriore trasferimento di dati personali in una maniera estremamente complessa e non trasparente. Spesso le persone non conoscono o non capiscono le modalità con cui vengono effettuate tali operazioni, chi raccoglie i loro dati o come esercitare un controllo. Un esempio di questo fenomeno è il monitoraggio delle attività di navigazione su Internet delle persone effettuato dai provider di reti di inserzioni tramite cookie o dispositivi analoghi al fine di inviare inserzioni mirate. Quando gli utenti visitano i siti Internet non si aspettano che un soggetto nascosto registri le loro visite e crei schede che li riguardano sulla base di informazioni che ne rivelano lo stile di vita, le preferenze o le antipatie.

70. D'altro canto, lo sviluppo stimola gli individui a condividere attivamente le loro informazioni personali, ad esempio sulle reti sociali. Sempre più giovani fanno parte di una rete sociale e interagiscono con i loro pari. Non si sa con certezza se queste persone (giovani) siano consapevoli dell'entità della diffusione dei dati che le riguardano e degli effetti a lungo termine delle loro azioni.

6.2. *Migliorare la trasparenza*

71. La trasparenza riveste un'enorme importanza in qualsiasi regime di protezione dei dati, non solo per il suo valore intrinseco, ma anche perché permette di esercitare altri principi di protezione dei dati. Le persone potranno esercitare i loro diritti solo se saranno a conoscenza del trattamento dei dati.

72. Molte disposizioni della direttiva 95/46/CE riguardano la trasparenza. Gli articoli 10 e 11 prevedono l'obbligo di fornire agli interessati informazioni sulla raccolta dei loro dati personali. L'articolo 12, inoltre, riconosce il diritto a ricevere una copia dei propri dati personali in forma intelligibile (diritto di accesso). L'articolo 15 riconosce il diritto di conoscere la logica in base alla quale vengono adottate decisioni automatizzate che producono effetti giuridici. Ultimo ma non meno importante aspetto, l'articolo 6, paragrafo 1, lettera a), conformemente al quale i dati devono essere trattati lealmente, comporta a sua volta un obbligo di trasparenza. I dati personali non possono essere trattati per motivi nascosti o segreti.

([37]) Cfr. l'articolo 27 del regolamento, (GU L 8 del 12.1.2001, pag. 1).

73. La comunicazione suggerisce di integrare un principio generale di trasparenza. In risposta a tale suggerimento il GEPD sottolinea che, come si può dedurre dalle varie disposizioni relative alla trasparenza indicate nel paragrafo precedente, il concetto di trasparenza è già parte integrante dell'attuale quadro giuridico sulla protezione dei dati, anche se in maniera implicita. A parere del GEPD, potrebbe avere valore aggiunto inserire un principio di trasparenza *esplicito*, collegato o meno alla disposizione esistente in materia di trattamento leale. Tale misura accrescerebbe la certezza del diritto e confermerebbe altresì che un responsabile deve trattare i dati personali in maniera trasparente in qualsiasi circostanza, non solo su richiesta o perché tenuto ad agire in tal senso sulla base di una determinata disposizione giuridica.

74. Tuttavia, è forse più importante rafforzare le disposizioni esistenti in materia di trasparenza, quali gli attuali articoli 10 e 11 della direttiva 95/46/CE. Tali disposizioni specificano gli elementi informativi che devono essere forniti, ma non sono precise sulle modalità. Più concretamente, il GEPD suggerisce di rafforzare le disposizioni esistenti prevedendo:

— l'obbligo per i responsabili di fornire informazioni sul trattamento dei dati facilmente accessibili e comprensibili e in un linguaggio chiaro e semplice ([38]). Le informazioni devono essere chiare, evidenti e visibili. La disposizione potrebbe altresì prevedere l'obbligo di garantire la facilità di comprensione delle informazioni. Tale obbligo sancirebbe l'illegalità delle politiche sulla vita privata che sono opache e di difficile comprensione,

— l'obbligo di fornire le informazioni in maniera semplificata e diretta agli interessati. Le informazioni devono inoltre essere consultabili in modo permanente e non scomparire da un mezzo elettronico dopo breve tempo. Tale disposizione permetterebbe agli utenti di conservare e riprodurre le informazioni in futuro, consentendo l'ulteriore accesso ai dati.

6.3. *Sostegno all'obbligo di notificare le violazioni della sicurezza*

75. Il GEPD è favorevole alla proposta della Commissione di introdurre nello strumento generale una disposizione sulla comunicazione delle violazioni di dati personali che estenda a tutti i responsabili del trattamento l'obbligo previsto per taluni fornitori nella direttiva e-Privacy rivista. Ai sensi della direttiva e-Privacy rivista l'obbligo si applica solo ai fornitori di servizi di comunicazione elettronica (fornitori di servizi di telefonia — servizi VoIP compresi — e di accesso a Internet). L'obbligo non contempla altri responsabili del trattamento dei dati. I motivi che giustificano l'obbligo si applicano appieno a responsabili del trattamento diversi dai fornitori di servizi di comunicazione elettronica.

76. La notifica delle violazioni della sicurezza persegue finalità differenti. La più ovvia, evidenziata dalla comunicazione, è quella di fungere da strumento di informazione per mettere al corrente gli interessati dei rischi ai quali sono esposti in caso di danneggiamento dei loro dati personali. In questo modo le persone avranno la possibilità di adottare le misure necessarie per mitigare tali rischi. Ad esempio, qualora vengano avvisati di violazioni riguardanti le loro informazioni finanziarie, gli interessati potranno, fra l'altro, procedere alla modifica delle password o alla cancellazione dei loro account. La notifica delle violazioni della sicurezza, inoltre, contribuisce all'effettiva applicazione di altri principi e obblighi sanciti dalla direttiva. Gli obblighi di notificare le violazioni della sicurezza, ad esempio, incentivano i responsabili del trattamento dei dati ad attuare misure di sicurezza più rigorose al fine di prevenire le violazioni. La notifica delle violazioni della sicurezza è inoltre uno strumento finalizzato ad accrescere la responsabilità dei responsabili del trattamento dei dati e, più in particolare, a rafforzare il rispetto degli obblighi loro incombenti (cfr. il capo 7). Infine, la notifica delle violazioni della sicurezza è uno strumento per l'applicazione della legge da parte delle autorità di protezione dei dati. La notifica di una violazione alle autorità di protezione dei dati può dare luogo a un'indagine sulle pratiche generali di un responsabile del trattamento dei dati.

77. Le norme specifiche sulle violazioni della sicurezza della direttiva e-Privacy rivista sono state oggetto di un ampio dibattito durante la fase parlamentare del quadro legislativo che ha preceduto l'adozione della direttiva e-Privacy. In tale dibattito sono stati presi in considerazione sia i pareri del Gruppo di lavoro articolo 29 e del GEPD che quelli di altre parti interessate. Le norme riflettono i pareri di attori differenti. Rappresentano un equilibrio di interessi: se, da una parte, i criteri da cui scaturisce l'obbligo di notificazione sono in linea di principio adeguati per la protezione delle persone, dall'altro assolvono la propria funzione senza imporre requisiti eccessivamente gravosi e inutili.

6.4. *Rafforzamento del consenso*

78. L'articolo 7 della direttiva sulla protezione dei dati elenca sei basi giuridiche per il trattamento dei dati personali. Il consenso è una di queste. Il trattamento dei dati personali da parte dei responsabili può essere effettuato nella misura in cui gli interessati abbiano dato il proprio consenso informato alla raccolta e all'ulteriore trattamento dei loro dati.

79. Nella pratica gli utenti hanno spesso un controllo limitato sui loro dati, in particolare negli ambienti tecnologici. Uno dei metodi che vengono talvolta utilizzati è il consenso implicito, ossia il consenso che è stato dedotto. Tale consenso può venire dedotto da un'azione compiuta dall'individuo (ad esempio l'azione consistente nell'utilizzare

([38]) Cfr. la pagina 6 della comunicazione.

un sito Internet viene ritenuta un atto di consenso alla registrazione dei dati dell'utente a fini commerciali). Può essere dedotto anche dal silenzio o dall'inazione (il mancato deselezionamento di una casella contrassegnata è ritenuto un consenso).

80. Ai sensi della direttiva, per risultare valido il consenso deve essere informato, libero e specifico. Deve essere una manifestazione di volontà informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento. Il modo in cui il consenso viene fornito deve essere univoco.

81. Il consenso che viene dedotto da un'azione e più precisamente dal silenzio o dall'inazione spesso non è un consenso univoco. Tuttavia, non è sempre possibile stabilire con chiarezza in che cosa consista un consenso vero e univoco. Alcuni responsabili del trattamento dei dati sfruttano questa incertezza affidandosi a metodi inadeguati per l'espressione di un consenso vero e univoco.

82. Alla luce delle precedenti considerazioni, il GEPD sostiene la Commissione in merito alla necessità di chiarire i limiti del consenso e di garantire che venga considerato tale solo il consenso costruito su basi solide. A tale proposito il GEPD formula i seguenti suggerimenti ([39]):

— si potrebbe valutare l'ipotesi di ampliare i casi in cui è necessario il consenso esplicito, attualmente limitato ai dati sensibili,

— adottare disposizioni supplementari per il consenso negli ambienti online,

— adottare disposizioni supplementari per il consenso al trattamento dei dati per finalità secondarie (ad esempio, casi in cui il trattamento è secondario al trattamento principale o non è ovvio),

— in un ulteriore strumento legislativo, adottato o meno dalla Commissione a norma dell'articolo 290 del TFUE, precisare il tipo di consenso necessario, ad esempio, specificare il livello di consenso in relazione al trattamento dei dati tramite le etichette RFID affisse ai prodotti di consumo o su altre tecniche specifiche.

6.5. *Portabilità dei dati e diritto all'oblio*

83. La portabilità dei dati e il diritto all'oblio sono due concetti interconnessi presentati dalla comunicazione per rafforzare i diritti degli interessati. Complementari ai principi già indicati nella direttiva, garantiscono all'interessato il diritto di opporsi all'ulteriore trattamento dei suoi dati personali e prevedono l'obbligo per il responsabile di cancellare le informazioni appena non sono più necessarie ai fini del trattamento.

84. Questi due nuovi concetti hanno valore aggiunto principalmente nel contesto di una società dell'informazione in cui sempre più dati vengono automaticamente immagazzinati e conservati per periodi di tempo indeterminati. L'esperienza dimostra che, anche qualora sia la parte interessata stessa a inserire i dati, il livello di controllo che quest'ultima ha effettivamente sui suoi dati personali è in pratica molto limitato, tanto più alla luce della memoria gigantesca rappresentata oggigiorno da Internet. Da un punto di vista economico, inoltre, per un responsabile del trattamento cancellare i dati risulta più dispendioso che conservarli. L'esercizio dei diritti personali va pertanto contro la tendenza economica naturale.

85. Sia la portabilità dei dati che il diritto all'oblio potrebbero contribuire a promuovere un riequilibrio a favore del soggetto interessato. Obiettivo della portabilità dei dati è permettere alle persone di avere un maggiore controllo sulle loro informazioni, mentre il diritto all'oblio garantisce la cancellazione automatica dei dati dopo un certo periodo di tempo, indipendentemente dall'iniziativa dell'interessato e dal fatto che fosse a conoscenza o meno dell'eventuale conservazione dei suoi dati personali.

86. Più precisamente, per portabilità dei dati s'intende la capacità degli utenti di modificare le preferenze relative al trattamento dei loro dati, riguardo in particolare a nuovi servizi tecnologici. Questo concetto si applica sempre più a servizi che prevedono la conservazione di informazioni, tra cui dati personali, quali la telefonia mobile, e a servizi che conservano immagini, email e altre informazioni, avvalendosi talvolta di servizi di cloud computing.

87. Le persone devono poter cambiare facilmente e liberamente fornitore e trasferire i loro dati personali a un altro fornitore di servizi. Il GEPD ritiene che i diritti attualmente sanciti nella direttiva 95/46/CE potrebbero essere rafforzati inserendo un diritto alla portabilità nel contesto dei servizi della società dell'informazione in particolare, al fine di assicurare agli individui che i fornitori e altri pertinenti responsabili del trattamento dei dati consentano loro di accedere alle informazioni personali che li riguardano garantendo al contempo che i vecchi fornitori o altri responsabili del trattamento cancellino tali dati anche qualora intendano conservarli per le loro legittime finalità.

88. La codificazione di un nuovo «diritto all'oblio» garantirebbe la cancellazione dei dati personali o il divieto del loro ulteriore utilizzo, senza un'azione necessaria da parte dell'interessato, ma a condizione che tali dati siano già stati conservati per un certo periodo di tempo. In altre parole, ai dati verrebbe attribuita una sorta di data di scadenza. Questo principio viene già affermato nelle sentenze nazionali o applicato in settori specifici, ad esempio

([39]) Attualmente il Gruppo di lavoro articolo 29 sta elaborando un parere sul «consenso». Da tale parere potrebbero scaturire ulteriori suggerimenti.

per i fascicoli di polizia, i casellari giudiziari o i fascicoli disciplinari: alcune leggi nazionali prevedono che i dati personali vengano automaticamente cancellati o non vengano ulteriormente utilizzati o diffusi, specialmente dopo un determinato periodo di tempo, senza la necessità di effettuare un'analisi preventiva caso per caso.

89. In tal senso il nuovo «diritto all'oblio» dovrebbe essere collegato alla portabilità dei dati. Grazie al valore aggiunto apportato da detta misura, l'interessato non dovrà adoperarsi o insistere per ottenere la cancellazione dei suoi dati personali, poiché questa avverrà in maniera oggettiva e automatica. Solo in circostanze molto precise, laddove sia possibile stabilire la specifica necessità di conservare le informazioni più a lungo, un responsabile del trattamento potrebbe essere autorizzato a conservare i dati. Questo «diritto all'oblio» invertirebbe pertanto l'onere della prova dall'interessato al responsabile del trattamento e costituirebbe un'impostazione predefinita a tutela della vita privata per il trattamento dei dati personali.

90. Il GEPD ritiene che il diritto all'oblio potrebbe rivelarsi particolarmente utile nel contesto dei servizi della società dell'informazione. L'obbligo di cancellare o di non diffondere ulteriormente le informazioni dopo un periodo di tempo determinato risulta utile soprattutto nell'ambito dei mezzi di comunicazione o di Internet, e in particolare nelle reti sociali. Sarebbe altrettanto utile per quanto riguarda le apparecchiature terminali: i dati conservati su computer o dispositivi mobili verranno automaticamente cancellati o bloccati dopo un periodo di tempo determinato, quando non saranno più in possesso della persona interessata. In tal senso il diritto all'oblio può tradursi in un obbligo di «privacy by design» (tutela della vita privata fin dalla progettazione).

91. In sintesi, il GEPD ritiene che la portabilità dei dati e il diritto all'oblio siano concetti utili. Potrebbe essere opportuno inserirli nello strumento giuridico, ma probabilmente limitandoli all'ambiente elettronico.

6.6. Trattamento dei dati personali dei minori

92. La direttiva 95/46/CE non contiene norme precise sul trattamento dei dati personali dei minori. Non viene pertanto riconosciuta la necessità di riservare ai minori una protezione particolare in casi specifici, in virtù sia della loro vulnerabilità sia dell'incertezza giuridica che ne deriva, in particolare nei seguenti settori:

— la raccolta dei dati dei minori e il modo in cui devono essere informati della raccolta,

— il modo in cui si ottiene il consenso dei minori. In assenza di norme specifiche sulle modalità di ottenimento del consenso dei minori e sull'età al di sotto della quale i minori devono essere considerati tali, dette questioni sono disciplinate dalla legislazione nazionale, che varia da uno Stato membro all'altro ([40]),

— le modalità e le condizioni alle quali i minori o i loro rappresentanti legali possono esercitare i loro diritti a norma della direttiva.

93. Il GEPD ritiene che gli interessi particolari dell'infanzia sarebbero meglio tutelati se il nuovo strumento giuridico contenesse disposizioni supplementari destinate specificamente alla raccolta e all'ulteriore trattamento dei dati dei minori. Tali disposizioni mirate garantirebbero inoltre la certezza del diritto in questo settore specifico e andrebbero a beneficio dei responsabili del trattamento dei dati, che attualmente devono rispettare requisiti giuridici diversi.

94. Il GEPD suggerisce di inserire nello strumento giuridico le seguenti disposizioni:

— l'obbligo di adeguare ai minori le informazioni in quanto tale misura permetterebbe loro di comprendere più facilmente che cosa comporta la raccolta di dati personali che li riguardano,

— l'obbligo di adeguare ai minori altri requisiti in materia di informazione, sul modo in cui devono essere fornite le informazioni e possibilmente anche sul contenuto,

— una misura specifica che tuteli i minori dalla pubblicità comportamentale,

— il rafforzamento del principio di limitazione delle finalità riguardo ai dati dei minori,

— il divieto di raccogliere alcune categorie di dati personali dei minori,

— la fissazione di una soglia d'età, al di sotto della quale in linea generale i dati dei minori devono essere raccolti solo con il consenso esplicito e verificabile dei genitori,

— qualora sia necessario ottenere il consenso dei genitori, occorrerà definire norme sulle modalità di accertamento dell'età del minore, che permettano in altre

([40]) Il consenso è solitamente collegato all'età in cui i minori possono assumere obblighi contrattuali, ovvero l'età in cui si presume che i minori abbiano raggiunto un certo livello di maturità. A norma della legislazione spagnola, ad esempio, è necessario il consenso dei genitori per la raccolta di dati riguardanti minori di età inferiore a 14 anni. Al di sopra di questa età i minori vengono ritenuti in grado di fornire il proprio consenso. Nel Regno Unito, la legge sulla tutela dei dati (Data protection Act) non indica un'età o a una soglia precisa. Tuttavia, secondo l'interpretazione fornita dall'Autorità di protezione dei dati del Regno Unito, i minori di età superiore a 12 anni possono fornire il proprio consenso. I minori al di sotto dei 12 anni di età, invece, non possono fornire il proprio consenso e, per ottenere i loro dati personali, occorre prima ricevere il permesso di un genitore o di un tutore.

parole di stabilire che la persona in questione è minorenne e di verificare il consenso dei genitori. Questo è un settore in cui l'UE può prendere spunto da altri paesi, come gli Stati Uniti ([41]).

6.7. *Meccanismi di ricorso collettivo*

95. Sarebbe inutile rafforzare la sostanza dei diritti delle persone senza prevedere meccanismi procedurali efficaci atti a garantire l'applicazione di tali diritti. A tale proposito, il GEPD raccomanda di inserire nella legislazione dell'UE meccanismi di ricorso collettivo per la violazione delle norme in materia di protezione dei dati. In particolare, i meccanismi di ricorso collettivo che autorizzano gruppi di cittadini a mettere in comune i ricorsi individuali nell'ambito di un'unica azione legale potrebbero costituire uno strumento molto efficace per facilitare l'applicazione delle norme di protezione dei dati ([42]). Anche le autorità di protezione dei dati si sono espresse a favore di questa innovazione nel documento del Gruppo di lavoro sul futuro della privacy.

96. Nei casi di minore impatto è improbabile che le vittime di una violazione delle norme di protezione dei dati propongano ricorsi individuali contro i responsabili del trattamento, considerati i costi, i ritardi, le incertezze, i rischi e gli oneri ai quali sarebbero esposti. Tali difficoltà potrebbero venire superate o considerevolmente attenuate se esistesse un sistema di ricorso collettivo, che autorizzasse le vittime delle violazioni a mettere in comune i ricorsi individuali nell'ambito di un'unica azione legale. Il GEPD è altresì favorevole ad autorizzare soggetti qualificati, quali associazioni di consumatori od organismi pubblici, ad avviare azioni per il risarcimento dei danni in nome e per conto delle vittime di violazioni delle norme di protezione dei dati. Tali azioni non dovrebbero pregiudicare il diritto degli interessati a proporre ricorsi individuali.

97. Le azioni collettive sono importanti non solo al fine di garantire un pieno risarcimento o altre azioni correttive, ma indirettamente svolgono anche una funzione di maggiore deterrenza. Il rischio di sostenere danni collettivi ingenti nell'ambito di tali azioni incentiverebbe in maniera esponenziale i responsabili del trattamento a garantire effettivamente il rispetto delle norme. A tale proposito, un rafforzamento dell'applicazione delle norme da parte dei privati tramite i meccanismi di ricorso collettivo integrerebbe l'applicazione delle norme da parte delle autorità pubbliche.

98. La comunicazione non prende posizione sull'argomento. Il GEPD è consapevole del dibattito attualmente in corso a livello europeo sull'introduzione di mezzi di ricorso collettivo dei consumatori. È altresì consapevole del rischio di eccessi che questi meccanismi possono comportare in base all'esperienza di altri sistemi giuridici. Ciononostante, considerati i vantaggi che apporterebbero, il GEPD ritiene che questi fattori non costituiscano argomentazioni sufficienti a respingerne o rinviarne l'introduzione nella legislazione in materia di protezione dei dati ([43]).

7. **Rafforzamento del ruolo delle organizzazioni/dei responsabili del trattamento dei dati**

7.1. *Generale*

99. Il GEPD è del parere che, oltre a rafforzare i diritti delle persone, uno strumento giuridico moderno per la protezione dei dati debba contenere gli strumenti necessari ad accrescere la responsabilità dei responsabili del trattamento. Più precisamente, il quadro deve prevedere incentivi affinché i responsabili del trattamento del settore privato o pubblico inseriscano proattivamente misure di protezione dei dati nelle loro attività. Tali strumenti sarebbero utili innanzitutto perché, come precedentemente affermato, gli sviluppi tecnologici hanno comportato un brusco incremento in termini di raccolta, utilizzo e ulteriore trasferimento di dati personali, con un conseguente aumento dei rischi per la vita privata e la protezione dei dati personali, che dovrebbero essere compensati in maniera efficace. In secondo luogo, il quadro attuale è privo — ad eccezione di alcune disposizioni ben definite (cfr. di seguito) — di tali strumenti e i responsabili del trattamento possono adottare un approccio *reattivo* alla protezione dei dati e alla vita privata, decidendo di agire solo dopo l'insorgere di un problema. Questo approccio trova riscontro nelle statistiche, che tra i problemi ricorrenti evidenziano prassi di scarso rispetto e perdite di dati.

100. Il GEPD ritiene che il quadro esistente non sia sufficiente a proteggere efficacemente i dati personali nelle condizioni attuali e future. Quanto maggiori sono i rischi, tanto più elevata è la necessità di attuare misure concrete che proteggano le informazioni a livello pratico e garantiscano una tutela efficace. Se queste misure proattive non verranno attuate *de facto*, continueranno probabilmente a verificarsi errori, incidenti e negligenze che metteranno a repentaglio la vita privata delle persone in questa società sempre più digitale. A tal fine, il GEPD propone le misure illustrate di seguito.

7.2. *Rafforzamento degli obblighi dei responsabili del trattamento dei dati*

101. Il GEPD raccomanda di inserire una nuova disposizione che preveda l'obbligo, per i responsabili del trattamento dei dati, di attuare misure appropriate ed efficaci per dare applicazione ai principi e agli obblighi dello strumento giuridico, e di dimostrarne su richiesta l'osservanza.

([41]) Negli USA, la normativa COPPA (Children's Online Privacy Protection Act) impone ai gestori di siti commerciali o di servizi online rivolti ai minori di 13 anni di ottenere il consenso dei genitori prima di procedere alla raccolta di dati personali e ai gestori di siti commerciali destinati al pubblico generale di essere effettivamente al corrente del fatto che i visitatori specifici sono minorenni.

([42]) Cfr. anche il parere del GEPD del 25 luglio 2007 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati, (GU C 255 del 27.10.2007, pag. 10).

([43]) Alcune legislazioni nazionali prevedono già meccanismi analoghi.

102. Questo tipo di disposizione non è del tutto nuovo. L'articolo 6, paragrafo 2, della direttiva 95/46/CE fa riferimento ai principi relativi alla qualità dei dati e afferma che «il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1». Analogamente, l'articolo 17, paragrafo 1, prevede che i responsabili del trattamento dei dati attuino misure di natura sia tecnica che organizzativa. Queste disposizioni, tuttavia, hanno una portata limitata. L'inserimento di una disposizione generale sulla responsabilità stimolerebbe i responsabili del trattamento ad attuare misure proattive che consentano di rispettare tutti gli elementi della legislazione in materia di protezione dei dati.

103. Una disposizione sulla responsabilità avrebbe la conseguenza di obbligare i responsabili del trattamento ad attuare meccanismi e sistemi di controllo interni che garantiscano il rispetto dei principi e dei requisiti del quadro. Ciò comporterebbe, ad esempio, il coinvolgimento dei vertici dirigenziali nelle politiche di protezione dei dati, la mappatura di procedure volte a garantire la corretta individuazione di tutte le operazioni di trattamento dei dati, la definizione di politiche di protezione dei dati vincolanti che dovrebbero anche essere costantemente rivedute e aggiornate al fine di contemplare nuove operazioni di trattamento dei dati, il rispetto dei principi di qualità, comunicazione, sicurezza, accesso, eccetera. Comporterebbe altresì la necessità, per i responsabili del trattamento, di conservare le prove al fine di dimostrare su richiesta alle autorità il rispetto delle disposizioni. In alcuni casi dovrebbe essere anche obbligatorio dimostrare l'osservanza delle norme alla collettività. Si potrebbe procedere in tal senso prevedendo ad esempio la necessità per i responsabili del trattamento di includere la protezione dei dati nelle relazioni pubbliche (annuali), qualora tali relazioni siano obbligatorie per altri motivi.

104. Ovviamente, le tipologie di misure interne ed esterne da attuare devono essere appropriate e dipendere dai fatti e dalle circostanze di ogni caso particolare. Esiste una notevole differenza tra il trattamento di alcune centinaia di dati di clienti consistenti unicamente in nomi e indirizzi e il trattamento di informazioni di milioni di pazienti, compresa la loro anamnesi, da parte del responsabile. Lo stesso ragionamento vale per i modi specifici in cui occorre valutare l'efficacia delle misure. Esiste un'esigenza di scalabilità.

105. Lo strumento giuridico generale globale di protezione dei dati non deve definire i requisiti specifici della responsabilità, ma solo i suoi elementi essenziali. La comunicazione prevede taluni elementi volti a rafforzare gli obblighi dei responsabili del trattamento dei dati, che il GEPD accoglie con grande favore. Più precisamente, il GEPD sostiene appieno la proposta di rendere obbligatori gli incaricati della protezione dei dati e le valutazioni d'impatto sulla privacy, al ricorrere di determinate condizioni soglia.

106. Il GEPD, inoltre, raccomanda di delegare alla Commissione i poteri previsti dall'articolo 290 del TFUE per integrare i requisiti di base necessari a soddisfare il criterio della responsabilità. L'utilizzo di questi poteri rafforzerebbe la certezza del diritto dei responsabili del trattamento e armonizzerebbe il rispetto della normativa in tutta l'UE. Per l'elaborazione di questi strumenti specifici dovranno essere consultati sia il Gruppo di lavoro articolo 29 sia il GEPD.

107. Infine, le misure concrete in materia di responsabilità che i responsabili del trattamento saranno tenuti ad attuare potrebbero essere imposte anche dalle autorità di protezione dei dati nell'ambito dei loro poteri di applicazione della normativa. A tal fine, alle autorità di protezione dei dati si dovrebbero conferire nuovi poteri che permettano loro di imporre misure correttive o sanzioni. A titolo di esempio, si dovrebbe prevedere lo sviluppo di programmi interni di conformità volti ad applicare il concetto di «privacy by design» (tutela della vita privata fin dalla progettazione) in prodotti e servizi specifici, eccetera. Misure correttive dovranno essere imposte solo nella misura in cui siano appropriate, proporzionate ed efficaci a garantire il rispetto delle norme giuridiche applicabili e vincolanti.

7.3. *Privacy by design (tutela della vita privata fin dalla progettazione)*

108. Il concetto di «privacy by design» si riferisce all'integrazione della protezione dei dati e della vita privata fin dalla progettazione di nuovi prodotti, servizi e procedure che comportano il trattamento di dati personali. Il GEPD ritiene che questo concetto sia un elemento del principio di responsabilità. Di conseguenza, i responsabili del trattamento dei dati saranno altresì tenuti a dimostrare di avere attuato, se del caso, questo principio. Recentemente, la 32ª conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata ha formulato una risoluzione in cui ha riconosciuto il concetto di «privacy by design» quale elemento essenziale della protezione fondamentale della vita privata ([44]).

109. La direttiva 95/46/CE contiene alcune disposizioni che incoraggiano l'applicazione di questo concetto ([45]), ma non riconosce espressamente tale obbligo. Il GEPD si compiace che la comunicazione approvi il principio di «privacy by design» quale strumento volto a garantire il rispetto delle norme di protezione dei dati. Suggerisce di includere una disposizione vincolante che preveda un obbligo di «privacy by design», che potrebbe basarsi sulla formulazione del considerando 46 della direttiva 95/46/CE. Per la precisione, la disposizione dovrà prevedere espressamente che i responsabili del trattamento attuino misure tecniche e organizzative, sia al momento

([44]) Risoluzione sul concetto di «privacy by design» (tutela della vita privata fin dalla progettazione), adottata dalla 32ª conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata, Gerusalemme, 27-29 ottobre 2010.

([45]) La direttiva comprende disposizioni che indirettamente, in situazioni diverse, richiedono l'attuazione del principio di «privacy by design». In particolare, l'articolo 17 prevede che i responsabili del trattamento attuino misure tecniche ed organizzative appropriate al fine di impedire il trattamento illecito dei dati personali. L'articolo 14, paragrafo 3, stabilisce che «all'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni».

della progettazione che a quello dell'esecuzione del trattamento, in particolare al fine di garantire la protezione dei dati personali e di impedirne qualsiasi trattamento non autorizzato ([46]).

110. Sulla base di tale disposizione i responsabili del trattamento dei dati saranno tenuti — tra l'altro — a garantire che i sistemi di trattamento siano concepiti in modo tale che venga trattato il minor numero di dati personali possibile, vengano attuate impostazioni predefinite a tutela della vita privata, ad esempio che nelle reti sociali venga mantenuta la riservatezza, in maniera predefinita, dei profili individuali e vengano attuati strumenti in grado di garantire agli utenti una maggiore protezione dei loro dati personali (ad esempio controllo degli accessi, cifratura).

111. I vantaggi di un riferimento più esplicito al concetto di «privacy by design» possono essere riassunti come segue:

— evidenzierebbe l'importanza del principio in sé, quale strumento volto a garantire che processi, prodotti e servizi siano concepiti fin dall'inizio nell'ottica della tutela della vita privata,

— diminuirebbe le violazioni della vita privata e ridurrebbe al minimo l'inutile raccolta di dati offrendo alle persone effettive possibilità di scelta riguardo ai loro dati personali,

— eviterebbe la necessità di ricorrere successivamente a soluzioni di ripiego nel tentativo di risolvere problemi ai quali potrebbe essere difficile, se non impossibile, porre rimedio,

— faciliterebbe inoltre l'effettiva applicazione e attuazione di questo principio da parte delle autorità di protezione dei dati.

112. Dall'effetto combinato di quest'obbligo scaturirà una domanda più sostenuta di prodotti e servizi di «privacy by design», che dovrebbe incentivare maggiormente l'industria a soddisfare tale richiesta. Si dovrebbe inoltre valutare l'ipotesi di creare un obbligo separato per i progettisti e i produttori di nuovi prodotti e servizi con una probabile incidenza sulla protezione dei dati e la vita privata. Il GEPD suggerisce di includere tale obbligo separato, che potrebbe agevolare ulteriormente il rispetto, da parte dei responsabili del trattamento dei dati, degli obblighi loro imposti.

113. La codificazione del concetto di «privacy by design» potrebbe essere integrata da una disposizione che ne enunci i requisiti generali applicabili in materia trasversale a vari settori, prodotti e servizi, garantendo ad esempio prerogative concrete agli utenti, da adottarsi conformemente a questo principio.

114. Il GEPD, inoltre, raccomanda di delegare alla Commissione i poteri previsti dall'articolo 290 del TFUE per integrare, se del caso, i requisiti di base necessari a soddisfare il criterio della «privacy by design» per prodotti e servizi specifici. L'utilizzo di questi poteri rafforzerebbe la certezza del diritto dei responsabili del trattamento e armonizzerebbe il rispetto della normativa in tutta l'UE. Per l'elaborazione di questi strumenti specifici dovranno essere consultati sia il Gruppo di lavoro articolo 29 sia il GEPD (cfr., nello stesso modo, il paragrafo 106 sulla responsabilità).

115. Infine, alle autorità di protezione dei dati dovrebbe essere conferito il potere di imporre misure correttive o sanzioni secondo restrizioni analoghe a quelle già indicate al punto 107, laddove i responsabili del trattamento dei dati abbiano chiaramente omesso di adottare misure concrete nei casi in cui avrebbero dovuto agire in tal senso.

7.4. *Servizi di certificazione*

116. La comunicazione riconosce la necessità di esaminare l'eventualità di creare regimi europei di certificazione per prodotti e servizi «ottemperanti ai principi di tutela della vita privata». Il GEPD sostiene appieno questo obiettivo e suggerisce di includere una disposizione che preveda la creazione di tali regimi e la loro possibile efficacia nell'UE, che potrebbe essere ulteriormente sviluppato in seguito in altri strumenti normativi. Questa misura dovrebbe integrare le disposizioni in materia di responsabilità e «privacy by design».

117. I regimi di certificazione volontari permetteranno di verificare l'attuazione, da parte di un responsabile del trattamento dei dati, di misure volte a ottemperare allo strumento giuridico. È inoltre probabile che i responsabili del trattamento dei dati — o anche i prodotti e i servizi — che beneficiano di un marchio di certificazione ottengano un vantaggio competitivo sugli altri. Tali regimi agevolerebbero altresì le attività di controllo e attuazione della legge delle autorità di protezione dei dati.

8. **Globalizzazione e diritto applicabile**

8.1. *Una evidente necessità di una protezione più coerente*

118. Come precedentemente indicato al capo 2, il trasferimento di dati personali oltre le frontiere dell'UE è aumentato in maniera esponenziale a seguito dello sviluppo di nuove tecnologie, del ruolo svolto dalle società multinazionali e della maggiore influenza esercitata dai governi nel trattamento e nella condivisione dei dati personali su scala internazionale. Questo è uno dei principali motivi che giustificano la revisione del quadro giuridico attuale. Di conseguenza, questo è uno dei settori in cui il GEPD chiede ambizione ed efficacia, alla luce dell'evidente necessità di garantire una protezione più coerente nel caso in cui i dati vengano trattati al di fuori dell'UE.

([46]) Nell'ambito del quadro attuale, il considerando 46 incoraggia i responsabili del trattamento dei dati ad attuare tali misure, ma ovviamente un considerando non ha carattere vincolante.

8.2. *Investire in norme internazionali*

119. Il GEPD ritiene che sia necessario investire maggiormente nello sviluppo di norme internazionali. Una maggiore armonizzazione del livello di protezione dei dati personali a livello globale chiarirebbe notevolmente la sostanza dei principi da rispettare e le condizioni per i trasferimenti dei dati. Obiettivo di queste norme globali sarà conciliare l'obbligo di garantire un livello elevato di protezione dei dati — compresi gli elementi essenziali di protezione dei dati dell'UE — con le specificità regionali.

120. Il GEPD sostiene l'ambizioso lavoro svolto finora nel quadro della conferenza internazionale dei commissari in materia di protezione dei dati per lo sviluppo e la divulgazione delle cosiddette «norme di Madrid», al fine di integrarle in uno strumento vincolante e possibilmente di avviare una conferenza intergovernativa ([47]). Il GEPD chiede alla Commissione di adottare le iniziative necessarie ad agevolare la realizzazione di questo obiettivo.

121. Il GEPD ritiene che sia inoltre importante garantire la coerenza tra questa iniziativa sulle norme internazionali, l'attuale riesame del quadro dell'UE sulla protezione dei dati e altri sviluppi quali l'attuale revisione delle linee guida dell'OCSE sulla protezione della vita privata e della Convenzione 108 del Consiglio d'Europa, che è aperta alla firma da parte dei paesi terzi (cfr. anche il punto 17). Il GEPD ritiene che la Commissione debba svolgere un ruolo specifico a tale proposito, indicando come promuoverà tale coerenza nei negoziati in seno all'OCSE e al Consiglio d'Europa.

8.3. *Chiarire i criteri di individuazione del diritto applicabile*

122. Poiché non sarà possibile raggiungere facilmente una piena coerenza, permarrà — almeno nel prossimo futuro — una certa diversità tra le legislazioni nazionali nell'UE e, a maggior ragione, oltre i confini dell'Unione. Il GEPD ritiene che un nuovo strumento giuridico dovrà chiarire i criteri di individuazione del diritto applicabile e garantire meccanismi semplificati per i flussi di dati nonché la responsabilità degli attori coinvolti nella circolazione dei dati.

123. Innanzitutto lo strumento giuridico dovrebbe garantire la possibilità di applicare il diritto dell'UE nei casi in cui i dati personali vengano trattati oltre i confini dell'Unione, sempre che la richiesta di applicare il diritto dell'UE sia giustificata. L'esempio di servizi di cloud computing non europei destinati a cittadini residenti nell'UE dimostra tale necessità. In un ambiente in cui i dati non sono conservati e trattati fisicamente in un luogo fisso, in cui utenti e fornitori di servizi dislocati in paesi diversi hanno capacità di esercitare un influenza concreta sui dati, è molto difficile individuare chi ha la responsabilità di rispettare quali principi di protezione dei dati. Vengono forniti orientamenti, specialmente dalle autorità di protezione dei dati, sulle modalità di interpretazione e applicazione della direttiva 95/46/CE nei casi in questione, ma gli orientamenti da soli non sono sufficienti a garantire la certezza del diritto in questo nuovo ambiente.

124. Nel territorio dell'UE la necessità di una maggiore precisione nel quadro giuridico e di un criterio semplificato per l'individuazione del diritto applicabile è stata sottolineata dal Gruppo di lavoro articolo 29 in un recente parere ([48]).

125. Il GEPD ritiene che sarebbe preferibile se lo strumento giuridico assumesse la forma di un regolamento da cui deriverebbero norme identiche applicabili in tutti gli Stati membri. Con un regolamento diventerebbe meno importante individuare il diritto applicabile. Questo è uno dei motivi per i quali il GEPD è fortemente favorevole all'adozione di un regolamento. Ciononostante, anche un regolamento lascerebbe un certo margine di manovra agli Stati membri. Se nel nuovo strumento verrà mantenuto un margine di manovra considerevole, il GEPD sosterrebbe la proposta, avanzata dal Gruppo di lavoro articolo 29, di passare da un'applicazione distributiva delle differenti legislazioni nazionali a un'applicazione centralizzata di un'unica legislazione in tutti gli Stati membri in cui ha sede un responsabile del trattamento dei dati. Chiede inoltre una cooperazione e un coordinamento maggiori tra le autorità di protezione dei dati nelle cause e nei reclami transnazionali (cfr. il capo 10).

8.4. *Semplificare i meccanismi di circolazione dei dati*

126. La necessità di coerenza e di un punto di riferimento di alto livello deve essere presa in considerazione non solo in merito ai principi globali di protezione dei dati, ma anche riguardo ai trasferimenti internazionali. Il GEPD sostiene appieno l'obiettivo della Commissione di semplificare le attuali procedure per i trasferimenti internazionali di dati e di assicurare un approccio più uniforme e coerente nei confronti dei paesi terzi e delle organizzazioni internazionali.

127. Il meccanismo di circolazione dei dati comprende sia trasferimenti del settore privato, in particolare tramite clausole contrattuali o «norme vincolanti d'impresa» (Binding Corporate Rules — BCR) che trasferimenti tra autorità pubbliche. Le norme vincolanti d'impresa sono uno degli elementi in cui sarebbe auspicabile adottare un approccio più coerente e semplificato. Il GEPD raccomanda di indicare espressamente le condizioni che disciplinano le BCR nel nuovo strumento giuridico ([49]):

— riconoscendo espressamente le norme vincolanti d'impresa quali strumenti che forniscono garanzie adeguate,

— illustrando gli elementi/le condizioni principali per l'adozione di norme vincolanti d'impresa,

([47]) Come suggerito dalla risoluzione sulle norme internazionali, adottata dalla 32ª conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata, Gerusalemme, 27-29 ottobre 2010.

([48]) Parere 8/2010 del Gruppo di lavoro articolo 29 sul diritto applicabile, WP 179.

([49]) Per quanto riguarda i trasferimenti internazionali cfr. anche il capo 8 del parere.

— definendo procedure di cooperazione per l'adozione di norme vincolanti d'impresa, compresi criteri per la scelta di un'autorità di controllo principale (sportello unico).

9. **Il settore della polizia e della giustizia**

9.1. *Lo strumento generale*

128. La Commissione ha ripetutamente sottolineato l'importanza di rafforzare la protezione dei dati nell'ambito delle attività di contrasto e prevenzione della criminalità, in cui lo scambio e l'utilizzo di dati personali è notevolmente aumentato. Anche il programma di Stoccolma, approvato dal Consiglio europeo, fa riferimento a una solida disciplina della protezione dei dati quale prerequisito principale per la strategia di gestione delle informazioni dell'UE in questo settore ([50]).

129. La revisione del quadro generale di protezione dei dati è l'occasione ideale per compiere progressi al riguardo, in particolare perché la comunicazione descrive giustamente la decisione quadro 2008/977 come inadeguata ([51]).

130. Il GEPD ha illustrato nella sezione 3.2.5 del presente parere i motivi che giustificano l'inclusione del settore della cooperazione di polizia e giudiziaria nello strumento generale. L'inclusione del settore della polizia e della giustizia apporta una serie di vantaggi aggiuntivi. Significa che le norme non si applicheranno più solo agli scambi transfrontalieri di dati ([52]), ma anche ai trattamenti di dati all'interno degli Stati membri. Verrà meglio garantita una protezione adeguata dello scambio di dati personali con i paesi terzi, anche per quanto riguarda gli accordi internazionali. Inoltre, le autorità di protezione dei dati avranno, nei confronti delle autorità giudiziarie e di polizia, gli stessi poteri ampi e armonizzati che hanno nei confronti di altri responsabili del trattamento dei dati. Infine, l'attuale articolo 13, che conferisce agli Stati membri il potere di adottare disposizioni legislative specifiche intese a limitare la portata degli obblighi e dei diritti previsti dallo strumento generale per interessi pubblici specifici, dovrà essere applicato con le stesse restrizioni vigenti in altri settori. In particolare, le garanzie specifiche previste dallo strumento generale in questo settore dovranno essere rispettate anche nella legislazione nazionale adottata nel settore della cooperazione di polizia e giudiziaria.

9.2. *Ulteriori norme specifiche per il settore della polizia e della giustizia*

131. Tale inclusione, tuttavia, non esclude norme e deroghe speciali, che tengano nella debita considerazione le specificità del settore, in linea con la dichiarazione 21 allegata al trattato di Lisbona. Possono essere previste restrizioni ai diritti degli interessati, che però devono essere necessarie, proporzionate e non modificare gli elementi essenziali del diritto stesso. A tale proposito occorre sottolineare che la direttiva 95/46/CE, compreso il suo articolo 13, attualmente disciplina le attività di contrasto in vari settori (ad esempio in ambito fiscale, doganale, antifrode) che non sono sostanzialmente differenti da molte funzioni svolte nel settore della polizia e della giustizia.

132. Devono inoltre essere previste misure di compensazione specifiche a favore delle persone interessate offrendo loro ulteriore protezione in un settore in cui il trattamento dei dati personali potrebbe essere più invasivo.

133. Alla luce delle precedenti considerazioni, il GEPD ritiene che il nuovo quadro debba contenere almeno gli elementi elencati di seguito, in linea con la Convenzione 108 e la raccomandazione R (87) 15:

— una distinzione tra le diverse categorie di dati e fascicoli in base al loro grado di esattezza e affidabilità, sostenendo il principio secondo cui i dati fondati su fatti dovrebbero essere differenziati da quelli fondati su opinioni o valutazioni personali,

— una distinzione tra le varie categorie di persone interessate (presunti criminali, vittime, testimoni, eccetera) e di fascicoli (temporanei, permanenti e informativi). Dovranno essere previste condizioni e garanzie specifiche per il trattamento di dati relativi a persone non sospette,

— meccanismi volti a garantire la verifica periodica e la rettifica al fine di salvaguardare la qualità dei dati trattati,

— potrebbero essere definite disposizioni e/o salvaguardie specifiche in relazione al trattamento dei dati biometrici e genetici (che sta acquisendo un peso sempre maggiore) nel settore dell'applicazione della legge. Il loro utilizzo dovrebbe essere limitato esclusivamente ai casi in cui non siano disponibili mezzi meno invasivi in grado di garantire lo stesso effetto ([53]),

— le condizioni per il trasferimento di dati personali ad autorità non competenti e a privati e per l'accesso e l'utilizzo ulteriore, da parte delle autorità di contrasto, di dati personali raccolti da privati.

([50]) Cfr. a tale proposito il parere del GEPD del 30 settembre 2010 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio — «Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia», punti 9-19.

([51]) Cfr. la sezione 3.2.5 sopra.

([52]) Attualmente questo è l'ambito di applicazione limitato della decisione quadro 2008/977.

([53]) A tale proposito, cfr. il documento del Gruppo di lavoro sul futuro della privacy, punto 112.

9.3. *Regimi settoriali di protezione dei dati*

134. La comunicazione afferma che «la decisione quadro non si sostituisce ai diversi atti normativi settoriali adottati a livello dell'Unione nei settori della cooperazione di polizia e giudiziaria in materia penale, in particolare a quelli che disciplinano il funzionamento di Europol, Eurojust, il sistema d'informazione Schengen (SIS) e il sistema informativo doganale (SID), contenenti anch'essi particolari disposizioni per la protezione dei dati e/o che fanno riferimento in linea generale a strumenti di protezione dei dati del Consiglio d'Europa».

135. A parere del GEPD, un nuovo quadro giuridico dovrebbe essere, per quanto possibile, chiaro, semplice e coerente. In presenza di un ampio numero di regimi differenti che disciplinano, ad esempio, il funzionamento di Europol, Eurojust, SIS e Prüm, il rispetto delle norme resta o addirittura diventa più complicato. Questo è uno dei motivi per cui il GEPD è favorevole a uno strumento giuridico globale per tutti i settori.

136. Il GEPD è tuttavia consapevole che l'allineamento delle norme di sistemi diversi richiederà un lavoro considerevole, che deve essere svolto con attenzione. Il GEPD ritiene che un approccio graduale, quale indicato nella comunicazione, abbia senso nella misura in cui l'impegno a garantire un elevato livello di protezione dei dati in maniera coerente ed effettiva resti chiaro e visibile. Più concretamente:

— in una prima fase, è opportuno rendere applicabile lo strumento giuridico generale sulla protezione dei dati a tutti i trattamenti nel settore della cooperazione di polizia e giudiziaria, compresi gli adeguamenti per la polizia e la giustizia (come definiti nella sezione 9.2),

— in una seconda fase, i regimi settoriali di protezione dei dati dovranno essere allineati a questo strumento generale. La Commissione deve impegnarsi ad adottare proposte per questa seconda fase, in tempi brevi e precisi.

10. **Le autorità di protezione dei dati e la cooperazione tra di esse**

10.1. *Rafforzare il ruolo delle autorità di protezione dei dati*

137. Il GEPD sostiene appieno l'obiettivo della Commissione di affrontare la questione dello status delle autorità di protezione dei dati e, più espressamente, di rafforzarne l'indipendenza, le risorse e i poteri di contrasto.

138. Il GEPD insiste inoltre sulla necessità di chiarire, nel nuovo strumento giuridico, il concetto essenziale di indipendenza delle autorità di protezione dei dati. La Corte di giustizia dell'Unione europea si è recentemente pronunciata in materia nella causa C-518/07 ([54]), in cui ha sottolineato che per indipendenza si intende l'assenza di qualsivoglia influenza esterna. Un'autorità di protezione dei dati può non sollecitare né accettare istruzioni da alcuno. Il GEPD suggerisce di codificare espressamente questi elementi di indipendenza nella legislazione.

139. Le autorità di protezione dei dati devono disporre delle risorse umane e finanziarie sufficienti per l'esercizio delle loro funzioni. Il GEPD suggerisce di includere questo requisito nella legislazione ([55]). Sottolinea infine la necessità di assicurare che le autorità siano dotate di poteri pienamente armonizzati per lo svolgimento delle loro funzioni di indagine e per l'imposizione di misure e sanzioni sufficientemente deterrenti e correttive. In questo modo verrebbe rafforzata la certezza del diritto sia per le persone interessate che per i responsabili del trattamento dei dati.

140. Il rafforzamento dell'indipendenza, delle risorse e dei poteri delle autorità di protezione dei dati deve andare di pari passo con una maggiore cooperazione a livello multilaterale, specialmente alla luce del crescente numero di questioni di protezione dei dati su scala europea. L'infrastruttura principale alla quale fare riferimento per tale cooperazione è ovviamente il Gruppo di lavoro articolo 29.

10.2. *Rafforzare il ruolo del Gruppo di lavoro*

141. L'esperienza dimostra che, da quando il gruppo è stato avviato nel 1997 ad oggi, il suo funzionamento si è evoluto. Ha acquisito una maggiore indipendenza e, nella pratica, non può più essere considerato come un semplice Gruppo di lavoro consultivo presso la Commissione. Il GEPD suggerisce di apportare ulteriori miglioramenti al funzionamento del Gruppo di lavoro, anche per quanto riguarda la sua infrastruttura e la sua indipendenza.

142. Il GEPD ritiene che la forza del gruppo sia intrinsecamente collegata all'indipendenza e ai poteri dei suoi membri. Nel nuovo quadro giuridico dovrà essere garantita l'autonomia del Gruppo di lavoro, conformemente ai criteri sviluppati per una completa indipendenza delle autorità di protezione dei dati dalla Corte di giustizia dell'Unione europea nella causa C-518/07. Il GEPD ritiene che il Gruppo di lavoro debba inoltre disporre della dotazione finanziaria e delle risorse sufficienti nonché di un segretariato rafforzato a sostegno dei suoi contributi.

143. Per quanto riguarda il segretariato del Gruppo di lavoro, il GEPD apprezza la sua integrazione nell'unità «protezione dei dati» della DG Giustizia, che offre al Gruppo di lavoro stesso il vantaggio di beneficiare di contatti efficienti e flessibili e di informazioni aggiornate sugli sviluppi in materia di protezione dei dati. D'altro canto, il GEPD mette in discussione il fatto che la Commissione (e più precisamente l'unità) sia al tempo stesso membro, segretariato e destinatario dei pareri del Gruppo di lavoro. Tale situazione giustificherebbe una maggiore indipendenza del segretariato. Il GEPD esorta la Commissione a valutare — in stretta consultazione con le parti interessate — il modo migliore di garantire tale indipendenza.

([54]) Causa C-518/07, *Commissione contro Germania*, non ancora pubblicata nella Raccolta.

([55]) Cfr., ad esempio, l'articolo 43, paragrafo 2, del regolamento (CE) n. 45/2001, che prevede tale requisito per il GEPD.

144. Infine, il rafforzamento dei poteri delle autorità di protezione dei dati richiede a sua volta il conferimento di maggiori poteri al Gruppo di lavoro, con una struttura che preveda norme e salvaguardie migliori e una maggiore trasparenza. Questi elementi dovranno essere sviluppati per il ruolo sia consultivo sia di contrasto del Gruppo di lavoro.

10.3. *Il ruolo consultivo del Gruppo di lavoro*

145. Le posizioni espresse dal Gruppo di lavoro nell'ambito del ruolo consultivo svolto presso la Commissione dovranno essere effettivamente attuate, in particolare per quanto riguarda l'interpretazione e l'applicazione dei principi della direttiva e di altri strumenti di protezione dei dati; in altre parole, occorrerà garantire l'autorevolezza delle posizioni del Gruppo di lavoro. Le autorità di protezione dei dati dovranno discutere ulteriormente la questione al fine di individuare il modo di includere questo aspetto nello strumento giuridico.

146. Il GEPD raccomanda soluzioni che renderebbero più autorevoli i pareri del Gruppo di lavoro senza modificarne sostanzialmente il funzionamento. Il GEPD suggerisce di includere l'obbligo, per le autorità di protezione dei dati e la Commissione, di tenere nel massimo conto i pareri e le posizioni comuni che ha adottato il Gruppo di lavoro, sulla base del modello utilizzato per le posizioni dell'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) ([56]). Il nuovo strumento giuridico, inoltre, potrebbe affidare al Gruppo di lavoro il compito esplicito di adottare «indirizzi interpretativi». Queste soluzioni alternative conferirebbero alle posizioni del Gruppo di lavoro un ruolo più forte, anche dinanzi ai tribunali.

10.4. *Applicazione coordinata da parte del Gruppo di lavoro*

147. Nell'ambito del quadro attuale, l'applicazione della normativa in materia di protezione dei dati negli Stati membri è di competenza delle 27 autorità di protezione dei dati, con uno scarso coordinamento per quanto riguarda la gestione di casi specifici. Nei casi in cui è coinvolto più di uno Stato membro o che hanno chiaramente una dimensione globale, invece, si assiste a una moltiplicazione dei costi per le imprese, che sono costrette a interagire con autorità pubbliche differenti per la stessa attività, e aumenta il rischio di un'applicazione incoerente: in circostanze eccezionali, le medesime attività di trattamento possono essere considerate legittime da un'autorità di protezione dei dati e vietate da un'altra.

148. Alcuni casi hanno una dimensione strategica che dovrebbe essere affrontata in maniera centralizzata. Il Gruppo di lavoro articolo 29 agevola le azioni di coordinamento e contrasto tra le autorità di protezione dei dati ([57]) in importanti questioni di protezione dei dati con implicazioni internazionali di questo tipo, com'è avvenuto nel caso delle reti sociali e dei motori di ricerca ([58]), nonché riguardo alle indagini coordinate in materia di telecomunicazioni e assicurazioni sanitarie svolte in differenti Stati membri.

149. Esistono tuttavia limitazioni alle azioni di contrasto che il Gruppo di lavoro può intraprendere nell'ambito del quadro attuale. Il Gruppo di lavoro può adottare posizioni comuni, ma non esistono strumenti in grado di garantire che tali posizioni vengano effettivamente attuate nella pratica.

150. Il GEPD suggerisce di includere nello strumento giuridico disposizioni supplementari che potrebbero sostenere l'applicazione coordinata delle norme di protezione dei dati, in particolare:

— l'obbligo di garantire che le autorità di protezione dei dati e la Commissione tengano nel massimo conto i pareri e le posizioni comuni che ha adottato il Gruppo di lavoro articolo 29 ([59]),

— l'obbligo, per le autorità di protezione dei dati, di collaborare lealmente sia l'una con l'altra che con la Commissione e il Gruppo di lavoro articolo 29 ([60]). Come esempio pratico di questa cooperazione leale, si potrebbe istituire una procedura mediante la quale le autorità di protezione dei dati informino la Commissione o il Gruppo di lavoro in caso di misure di applicazione delle normative nazionali con un elemento transfrontaliero, analoga alla procedura applicabile nell'ambito del quadro attuale riguardo alle decisioni di adeguatezza nazionali,

— precisazione delle regole di voto al fine di aumentare l'impegno delle autorità di protezione dei dati ad attuare le decisioni del Gruppo di lavoro. Si potrebbe stabilire che il Gruppo di lavoro prenda decisioni su base consensuale e che, nell'impossibilità di raggiungere un consenso, adotti decisioni di esecuzione solo

([56]) Regolamento (CE) n. 1211/2009 del Parlamento europeo e del Consiglio, del 25 novembre 2009, che istituisce l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) e l'Ufficio, (GU L 337 del 18.12.2009, pag. 1).

([57]) Oltre al Gruppo di lavoro articolo 29, la conferenza europea dei commissari per la protezione dei dati ha creato, circa dieci anni fa, un workshop permanente al fine di trattare i reclami transfrontalieri in maniera coordinata. Benché questo workshop presenti un innegabile valore aggiunto in termini di scambio di personale tra le autorità di protezione dei dati e offra una rete affidabile di punti di contatto, non può essere considerato un meccanismo di coordinamento per il processo decisionale.

([58]) Cfr. le lettere del Gruppo di lavoro articolo 29 del 12 maggio 2010 e del 26 maggio 2010, pubblicate sul sito Internet del Gruppo di lavoro articolo 29 (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Come indicato in precedenza, il regolamento (CE) n. 1211/2009 definisce un obbligo simile che precisa il ruolo dell'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC).

([60]) Cfr., a tale proposito, l'articolo 3 del regolamento (CE) n. 1211/2009, menzionato in precedenza.

con una maggioranza qualificata. Inoltre, un considerando potrebbe stabilire che le autorità di protezione dei dati che esprimono un voto positivo su un documento siano tenute ad attuarlo a livello nazionale o assumano un impegno politico in tal senso.

151. Il GEPD desidera esprimere le proprie riserve in merito all'introduzione di misure più forti, quali il conferimento di un valore vincolante alle posizioni del Gruppo di lavoro articolo 29. In questo modo verrebbe pregiudicata l'indipendenza delle singole autorità di protezione dei dati, che deve essere garantita dagli Stati membri ai sensi della legislazione nazionale. Qualora le decisioni del Gruppo di lavoro avessero un impatto diretto su terzi quali i responsabili del trattamento dei dati, sarebbe necessario prevedere nuove procedure tra cui salvaguardie come meccanismi di trasparenza e ricorso, compresa la possibilità di adire la Corte di giustizia dell'Unione europea.

10.5. *Cooperazione tra il GEPD e il Gruppo di lavoro*

152. Si potrebbero inoltre affinare le modalità di cooperazione tra il GEPD e il Gruppo di lavoro. Il GEPD è membro del Gruppo di lavoro e, al suo interno, contribuisce alle posizioni sui principali sviluppi strategici dell'UE, garantendone al contempo la coerenza con i propri pareri. Il GEPD rileva il crescente aumento, nel settore sia privato che pubblico, delle questioni inerenti alla vita privata che hanno implicazioni a livello nazionale in molti Stati membri e riguardo alle quali il Gruppo di lavoro può svolgere un ruolo specifico.

153. Il GEPD svolge un ruolo consultivo complementare per quanto riguarda gli sviluppi nel contesto dell'UE, che deve essere mantenuto. In qualità di organismo europeo, esercita questa competenza consultiva nei confronti delle istituzioni dell'UE nello stesso modo in cui le autorità nazionali di protezione dei dati forniscono consulenza ai loro governi.

154. Il GEPD e il Gruppo di lavoro operano da una prospettiva differente ma complementare. Per tali motivi è necessario mantenere e forse migliorare il coordinamento tra il Gruppo di lavoro e il GEPD, al fine di garantirne la collaborazione sulle principali questioni di protezione dei dati, ad esempio tramite il coordinamento periodico dei programmi di lavoro ([61]) e assicurando la trasparenza su questioni che hanno una dimensione più nazionale o riguardano un aspetto più specifico a livello dell'UE.

155. Nella direttiva attuale il coordinamento non viene menzionato per il semplice motivo che all'epoca dell'adozione della direttiva il GEPD non esisteva, ma a sei anni dalla sua creazione le complementarità del GEPD e del Gruppo di lavoro sono visibili e potrebbero essere riconosciute formalmente. Il GEPD ricorda che, ai sensi del regolamento (CE) n. 45/2001, ha la funzione di collaborare con le autorità nazionali di protezione dei dati e di partecipare alle attività del Gruppo di lavoro. Il GEPD raccomanda di fare espressamente riferimento alla cooperazione nel nuovo strumento giuridico e di strutturarla, se del caso, definendo ad esempio una procedura per la cooperazione.

10.6. *Cooperazione tra il GEPD e le autorità di protezione dei dati nel controllo dei sistemi UE*

156. Queste considerazioni si applicano anche a settori in cui è necessario coordinare il controllo tra il livello europeo e nazionale. È il caso degli organismi UE che trattano considerevoli quantità di dati forniti dalle autorità nazionali o dei sistemi d'informazione su vasta scala con una componente europea e nazionale.

157. Il sistema che disciplina attualmente alcuni sistemi d'informazione su vasta scala e organismi dell'UE — Europol, Eurojust e il Sistema d'informazione Schengen di prima generazione (SIS), ad esempio, sono dotati di autorità di controllo comuni con rappresentanti delle autorità nazionali di protezione dei dati — è un residuo della cooperazione intergovernativa dell'epoca pre-Lisbona e non rispetta la struttura istituzionale dell'UE di cui Europol ed Eurojust sono ora parte integrante, e in cui è stato ormai integrato anche «l'acquis di Schengen» ([62]).

158. La comunicazione annuncia che nel 2011 la Commissione avvierà una consultazione delle parti interessate sulla revisione di questi sistemi di controllo. Il GEPD esorta la Commissione a prendere quanto prima (in tempi brevi e precisi, come indicato in precedenza) una posizione nella discussione attualmente in corso in materia di controllo. Nell'ambito di tale discussione il GEPD assumerà la posizione illustrata di seguito.

159. In primo luogo occorre garantire che tutte le autorità di controllo soddisfino i criteri indispensabili dell'indipendenza, delle risorse e dei poteri di contrasto. È inoltre necessario fare in modo che vengano prese in considerazione le prospettive e le competenze esistenti a livello dell'UE. Questo significa che la cooperazione deve avvenire non solo tra le autorità nazionali, ma anche con l'autorità europea di protezione dei dati (attualmente il GEPD). Il GEPD ritiene che sia necessario seguire un modello che soddisfi tali requisiti ([63]).

160. Negli ultimi anni è stato sviluppato il modello di «controllo coordinato». Questo modello di controllo, attualmente operativo a livello di Eurodac e di parti del sistema informativo doganale, sarà presto esteso al sistema di informazione visti (VIS) e al Sistema d'informazione Schengen di seconda generazione (SIS II). Questo modello si articola su tre livelli: (1) il controllo a livello nazionale è

([61]) Ad esempio sulla base dell'inventario delle attività legislative pubblicato annualmente e aggiornato periodicamente, che è disponibile sul sito Internet del GEPD.

([62]) Ai sensi del regolamento (CE) n. 45/2001, il GEPD ha il dovere di collaborare con questi organismi.

([63]) Per quanto riguarda Eurojust, un modello deve anche prevedere che il controllo della protezione dei dati rispetti l'indipendenza della magistratura, nella misura in cui Eurojust tratti i dati nell'ambito dei procedimenti penali.

garantito dalle autorità di protezione dei dati; (2) il controllo a livello dell'UE è garantito dal GEPD; (3) il coordinamento è garantito da riunioni periodiche convocate dal GEPD, che agisce da segretariato di questo meccanismo di coordinamento. Questo modello si è rivelato efficace ed effettivo e in futuro dovrebbe essere previsto per altri sistemi di informazione.

C. **COME MIGLIORARE L'APPLICAZIONE DEL QUADRO ATTUALE?**

11. **Il breve periodo**

161. Durante il processo di revisione occorrerà impegnarsi per garantire la piena ed effettiva attuazione delle norme esistenti. Tali norme continueranno a essere applicabili finché il quadro futuro non verrà adottato e successivamente recepito negli ordinamenti nazionali degli Stati membri. In questo senso possono essere individuate varie linee d'azione.

162. Innanzitutto, la Commissione deve continuare a controllare il rispetto, da parte degli Stati membri, della direttiva 95/46/CE e, se del caso, avvalersi dei poteri conferitile dall'articolo 258 del TFUE. Recentemente sono stati avviati procedimenti di infrazione per l'errata attuazione dell'articolo 28 della direttiva riguardo al requisito dell'indipendenza delle autorità di protezione dei dati ([64]). La piena osservanza della direttiva deve essere controllata e assicurata anche in altri settori ([65]). Il GEPD, pertanto, accoglie con favore e sostiene appieno l'impegno di attuare una politica attiva contro le infrazioni assunto dalla Commissione nella comunicazione. La Commissione deve inoltre proseguire il dialogo strutturale con gli Stati membri in materia di attuazione ([66]).

163. In secondo luogo, occorre incoraggiare l'applicazione a livello nazionale al fine di garantire l'attuazione pratica delle norme di protezione dei dati, anche per quanto riguarda i nuovi fenomeni tecnologici e attori globali. Le autorità di protezione dei dati devono utilizzare appieno i loro poteri d'indagine e sanzionatori. È inoltre importante che gli attuali diritti degli interessati, in particolare il diritto di accesso, siano pienamente rispettati nella pratica.

164. In terzo luogo, nel breve periodo sembra necessario un maggiore coordinamento nell'applicazione delle norme. Il Gruppo di lavoro articolo 29 e i suoi documenti interpretativi svolgono un ruolo cruciale in tal senso, ma anche le autorità di protezione dei dati devono adoperarsi per la loro attuazione pratica. Occorre evitare conclusioni divergenti in relazione a casi aventi dimensione europea e globale; approcci comuni possono e devono essere raggiunti nell'ambito del Gruppo di lavoro. Indagini coordinate a livello UE sotto l'egida del Gruppo di lavoro possono a loro volta apportare un notevole valore aggiunto.

165. In quarto luogo, i principi di protezione dei dati devono essere proattivamente «integrati» nelle nuove normative che possono incidere, direttamente o indirettamente, sulla protezione dei dati. A livello UE, il GEPD compie sforzi considerevoli per contribuire al miglioramento della legislazione europea e tale impegno deve essere profuso anche a livello nazionale. Le autorità di protezione dei dati devono pertanto utilizzare appieno i loro poteri consultivi per garantire l'adozione di un approccio proattivo in tal senso. Le autorità di protezione dei dati, compreso il GEPD, possono svolgere un ruolo attivo anche nel controllo degli sviluppi tecnologici. L'attività di controllo è importante al fine di individuare precocemente le tendenze emergenti, evidenziare le possibili implicazioni per la protezione dei dati, sostenere soluzioni che tengano conto della protezione dei dati e sensibilizzare le parti interessate.

166. È infine necessario perseguire attivamente una maggiore cooperazione tra i vari attori a livello internazionale. È pertanto importante rafforzare gli strumenti internazionali di cooperazione. Iniziative quali le norme di Madrid e il lavoro attualmente in corso in seno al Consiglio d'Europa e all'OCSE meritano pieno sostegno. In tale contesto è molto positivo che la Commissione federale per il commercio degli USA (US Federal Trade Commission) sia ora entrata a far parte della famiglia dei commissari in materia di protezione dei dati e della vita privata nel quadro della loro conferenza internazionale.

D. **CONCLUSIONI**

OSSERVAZIONI GENERALI

167. Il GEPD accoglie con favore la comunicazione della Commissione in generale, poiché è convinto che sia necessario rivedere l'attuale quadro giuridico sulla protezione dei dati al fine di garantire una tutela efficace in una società dell'informazione destinata a svilupparsi ulteriormente e a diventare sempre più globalizzata.

168. La comunicazione individua le questioni e le sfide principali. Il GEPD condivide il parere della Commissione secondo cui in futuro continuerà a essere necessario disporre di un solido sistema di protezione dei dati, partendo dal presupposto che gli attuali principi generali di protezione dei dati continueranno a rimanere validi in una società che è sottoposta a profonde trasformazioni. Il GEPD condivide l'affermazione della comunicazione secondo cui le sfide sono enormi e sottolinea che, di conseguenza, le soluzioni proposte devono essere altrettanto ambiziose e rafforzare l'efficacia della protezione. Chiede pertanto di adottare un approccio più ambizioso su una serie di punti.

169. Il GEPD sostiene appieno l'approccio globale alla protezione dei dati. Si rammarica tuttavia che la comunicazione escluda dallo strumento generale taluni settori, quali il trattamento dei dati da parte delle istituzioni e degli organismi dell'UE. Il GEPD esorta la Commissione — nel

([64]) Cfr. la causa C-518/07, menzionata in precedenza, e il comunicato stampa della Commissione del 28 ottobre 2010 (IP/10/1430).

([65]) La Commissione ha avviato un procedimento di infrazione nei confronti del Regno Unito per l'asserita violazione di varie disposizioni in materia di protezione dei dati, tra cui il requisito della riservatezza delle comunicazioni elettroniche in merito alla pubblicità comportamentale. Cfr. il comunicato stampa della Commissione del 9 aprile 2009 (IP/09/570).

([66]) Cfr. la prima relazione della Commissione sull'applicazione della direttiva sulla protezione dei dati, menzionata in precedenza, pag. 22 e segg.

caso in cui dovesse decidere di tralasciare questi settori — ad adottare una proposta a livello dell'UE nel più breve tempo possibile e preferibilmente entro la fine del 2011.

PRINCIPALI PROSPETTIVE

170. Per il GEPD i punti di partenza del processo di revisione sono i seguenti:

— le misure di protezione dei dati devono, per quanto possibile, sostenere attivamente anziché ostacolare altri interessi legittimi (quali l'economia europea, la sicurezza delle persone e la responsabilità dei governi),

— i principi generali di protezione dei dati non devono e non possono essere modificati,

— tra gli obiettivi principali della revisione deve figurare una maggiore armonizzazione,

— la prospettiva dei diritti fondamentali deve costituire un elemento centrale del processo di revisione. Un diritto fondamentale ha come scopo la tutela dei cittadini in qualsiasi circostanza,

— il settore della polizia e della giustizia deve essere incluso nel nuovo strumento giuridico,

— il nuovo strumento giuridico deve essere formulato, per quanto possibile, in maniera tecnologicamente neutra e deve essere finalizzato a creare certezza del diritto più a lungo termine.

ELEMENTI DI UN NUOVO QUADRO

Armonizzazione e semplificazione

171. Il GEPD accoglie con favore l'impegno della Commissione a esaminare i mezzi per conseguire una maggiore armonizzazione delle norme di protezione dei dati a livello dell'UE. Il GEPD individua i settori in cui è urgente una maggiore e migliore armonizzazione: definizioni, le basi giuridiche del trattamento dei dati, diritti delle persone interessate, trasferimenti internazionali e autorità di protezione dei dati.

172. Il GEPD suggerisce di valutare le seguenti alternative per semplificare e/o ridurre l'ambito di applicazione degli obblighi in materia di notificazione:

— limitare l'obbligo di notificazione a specifiche tipologie di trattamento dei dati che comportano rischi specifici,

— un semplice obbligo di registrazione che preveda la registrazione da parte dei responsabili del trattamento (anziché la registrazione dettagliata di tutte le operazioni di trattamento dei dati),

— l'introduzione di un modulo di notifica uniforme per tutta l'UE.

173. Il GEPD ritiene che un regolamento, uno strumento unico che sia direttamente applicabile negli Stati membri, sia il mezzo più efficace per proteggere il diritto fondamentale alla protezione dei dati e raggiungere una maggiore convergenza nel mercato interno.

Rafforzare i diritti delle persone

174. Il GEPD è favorevole alla proposta di rafforzare i diritti delle persone avanzata nella comunicazione e formula i seguenti suggerimenti:

— nello strumento giuridico potrebbe essere integrato un principio di trasparenza. Tuttavia, è più importante rafforzare le disposizioni esistenti in materia di trasparenza (quali gli attuali articoli 10 e 11 della direttiva 95/46/CE),

— nello strumento generale potrebbe essere introdotta una disposizione sulla comunicazione delle violazioni di dati personali che estenda a tutti i responsabili del trattamento l'obbligo previsto per taluni fornitori nella direttiva e-Privacy rivista,

— i limiti del consenso devono essere chiariti. Si dovrebbe valutare l'ipotesi di ampliare i casi in cui è necessario il consenso esplicito nonché adottare disposizioni supplementari per gli ambienti online,

— devono essere introdotti diritti supplementari quali la portabilità dei dati e il diritto all'oblio, specialmente per i servizi della società dell'informazione su Internet,

— i diritti dell'infanzia devono essere meglio tutelati con una serie di disposizioni supplementari destinate specificamente alla raccolta e all'ulteriore trattamento dei dati dei minori,

— nella legislazione dell'UE devono essere introdotti meccanismi di ricorso collettivo per la violazione delle norme in materia di protezione dei dati volti ad autorizzare soggetti qualificati ad avviare azioni a nome di gruppi di cittadini.

Rafforzamento degli obblighi delle organizzazioni/dei responsabili del trattamento dei dati

175. Il nuovo quadro deve prevedere incentivi affinché i responsabili del trattamento inseriscano proattivamente misure di protezione dei dati nelle loro attività. Il GEPD propone l'introduzione di disposizioni generali in materia di responsabilità e di «privacy by design» (tutela della vita privata fin dalla progettazione). Dovrebbe altresì essere introdotta una disposizione sui regimi di certificazione nel campo della tutela della vita privata.

Globalizzazione e diritto applicabile

176. Il GEPD sostiene l'ambizioso lavoro svolto nel quadro della conferenza internazionale dei commissari in materia di protezione dei dati per lo sviluppo delle cosiddette «norme di Madrid», al fine di integrarle in uno strumento vincolante e possibilmente di avviare una conferenza intergovernativa. Il GEPD chiede alla Commissione di adottare misure concrete in tal senso in stretta collaborazione con l'OCSE e con il Consiglio d'Europa.

177. Un nuovo strumento giuridico dovrà chiarire i criteri di individuazione del diritto applicabile. Occorrerà garantire che i dati trattati oltre i confini dell'Unione europea non sfuggano all'applicazione del diritto dell'UE, laddove sussistano motivi giustificati per applicare tale diritto. Se il quadro giuridico assumesse la forma di un regolamento esisterebbero norme identiche in tutti gli Stati membri e diventerebbe meno importante individuare il diritto applicabile (all'interno dell'UE).

178. Il GEPD sostiene appieno l'obiettivo di assicurare un approccio più uniforme e coerente con riferimento ai paesi terzi e delle organizzazioni internazionali. Nello strumento giuridico dovrebbero essere incluse «norme vincolanti d'impresa» (Binding Corporate Rules — BCR).

Il settore della polizia e della giustizia

179. Uno strumento globale in cui sia contemplata l'inclusione della polizia e della giustizia potrà prevedere norme speciali, che tengano nella debita considerazione le specificità del settore, in linea con la dichiarazione 21 allegata al trattato di Lisbona. Dovranno essere previste misure di compensazione specifiche a favore delle persone interessate offrendo loro ulteriore protezione in un settore in cui il trattamento dei dati personali è per natura più invasivo.

180. Il nuovo quadro giuridico dovrà essere, per quanto possibile, chiaro, semplice e coerente. Occorre evitare il proliferare di regimi differenti, quali ad esempio quelli che disciplinano il funzionamento di Europol, Eurojust, SIS e Prüm. Il GEPD è consapevole che l'allineamento delle norme di sistemi diversi dovrà essere svolto in maniera attenta e graduale.

Le autorità di protezione dei dati e la cooperazione tra di esse

181. Il GEPD sostiene pienamente l'obiettivo della Commissione di affrontare la questione dello status delle autorità di protezione dei dati e di rafforzarne l'indipendenza, le risorse e i poteri di contrasto. Il GEPD raccomanda di:

— codificare, nel nuovo strumento giuridico, il concetto essenziale di indipendenza delle autorità di protezione dei dati, quale specificato dalla Corte di giustizia dell'Unione europea,

— stabilire nella legislazione che le autorità di protezione dei dati devono disporre di risorse sufficienti,

— conferire alle autorità poteri d'indagine e sanzionatori armonizzati.

182. Il GEPD suggerisce di apportare ulteriori miglioramenti al funzionamento del Gruppo di lavoro articolo 29, anche per quanto riguarda la sua indipendenza e la sua infrastruttura. Il Gruppo di lavoro deve inoltre disporre di risorse sufficienti e di un segretariato rafforzato.

183. Il GEPD suggerisce di rafforzare il ruolo consultivo del Gruppo di lavoro introducendo l'obbligo, per le autorità di protezione dei dati e la Commissione, di *tenere nel massimo conto i pareri e le posizioni comuni* che ha adottato il Gruppo di lavoro. Il GEPD é contrario al conferimento di valore vincolante alle posizioni del Gruppo di lavoro, in particolare perché in questo modo verrebbe pregiudicata l'indipendenza delle singole autorità di protezione dei dati. Il Garante europeo della protezione dei dati raccomanda alla Commissione di introdurre nel nuovo strumento giuridico disposizioni specifiche volte a rafforzare la cooperazione con il GEPD.

184. Il GEPD esorta la Commissione a prendere quanto prima una posizione sulla questione del controllo dei sistemi d'informazione su vasta scala e degli organismi dell'UE, tenendo conto che tutte le autorità di controllo devono soddisfare i criteri indispensabili dell'indipendenza, delle risorse sufficienti e dei poteri di contrasto e che occorre garantire che la prospettiva dell'UE sia ben rappresentata. Il GEPD sostiene il modello di «controllo coordinato».

Miglioramenti nell'ambito del sistema attuale:

185. Il GEPD incoraggia la Commissione a:

— continuare a controllare il rispetto, da parte degli Stati membri, della direttiva 95/46/CE e, se del caso, avvalersi dei poteri conferitile dall'articolo 258 del TFUE,

— promuovere l'applicazione a livello nazionale e il coordinamento in fase di applicazione,

— integrare proattivamente i principi di protezione dei dati nei nuovi regolamenti che possono incidere, direttamente o indirettamente, sulla protezione dei dati,

— perseguire attivamente una maggiore cooperazione tra i vari attori a livello internazionale.

Fatto a Bruxelles, il 14 gennaio 2011.

Peter HUSTINX

Garante europeo della protezione dei dati