COMMISSIONE EUROPEA

Bruxelles, 4.11.2010
COM(2010) 609 definitivo

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

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

1. LE NUOVE SFIDE

La direttiva del 1995[1] è una pietra miliare nella storia della protezione dei dati personali nell'Unione europea. Essa sancisce due antiche ambizioni ugualmente importanti del processo d'integrazione europea: la tutela dei diritti e delle libertà fondamentali delle persone, quindi anche del diritto fondamentale alla protezione dei dati, e la realizzazione del mercato interno, ossia, nello specifico, la libera circolazione dei dati personali.

A distanza di quindici anni questo duplice obiettivo ha mantenuto la sua validità e i principi che hanno trovato espressione nella direttiva restano saldi. **Eppure, la rapidità dell'evoluzione tecnologica e la globalizzazione hanno mutato profondamente il mondo in cui viviamo, ponendo nuove sfide alla protezione dei dati personali.**

Oggi la tecnologia consente di condividere agevolmente informazioni sui comportamenti e sulle preferenze, e di rendere pubblici a livello mondiale quantità di dati senza precedenti. I social network, con centinaia di milioni di membri in tutto il mondo, sono forse la più evidente ma di certo non l'unica manifestazione di questo fenomeno. Anche il cosiddetto cloud computing – tecnologie informatiche che permettono l'utilizzo di risorse software distribuite su server remoti – costituiscono una sfida per la protezione dei dati in quanto comportano il rischio che l'utente perda il controllo delle informazioni potenzialmente sensibili che avrà salvato su programmi ospitati nell'hardware di una terza persona. Secondo uno studio recente, le autorità di protezione dei dati, le organizzazioni professionali e le associazioni di consumatori sembrano concordare sul fatto che i rischi per la privacy e la protezione dei dati personali associati alle attività on line sono in aumento[2].

Allo stesso tempo **le modalità di raccolta dei dati personali si complicano e diventa più difficile individuarle**. Strumenti sofisticati consentono, ad esempio, agli operatori economici di monitorare il comportamento dei potenziali acquirenti così da adattare l'offerta. Il ricorso sempre più generalizzato alla raccolta automatizzata dei dati - vendita elettronica di titoli di trasporto, telepedaggio o dispositivi di localizzazione geografica – rende le persone più facilmente localizzabili solo perché si servono di apparecchiature mobili. Anche i poteri pubblici fanno ampio uso di dati personali per scopi diversi: rintracciare persone quando scoppia una malattia contagiosa, prevenire e combattere più efficacemente il terrorismo e la

---

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

2 Cfr. uno studio del luglio 2010 sui vantaggi economici delle tecnologie di rafforzamento della tutela della vita privata (*Study on the economic benefits of privacy enhancing technologies*, London Economics, July 2010)(http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), pag. 14

criminalità, gestire i regimi di sicurezza sociale, oppure per fini fiscali, nel contesto dell'*e-government* ecc.

A fronte di tutto ciò sorge inevitabilmente la domanda: le norme di protezione dei dati dell'Unione sono in grado di raccogliere ancora in modo adeguato ed efficace tali sfide?

Per rispondere a questa domanda la Commissione ha lanciato la revisione dell'attuale quadro giuridico con una conferenza di alto livello nel maggio 2009, cui hanno fatto seguito una consultazione pubblica conclusasi alla fine del 2009[3] e tutta una serie di studi[4].

Gli esiti di tali studi e consultazioni confermano che restano validi i principi fondamentali della direttiva e che è opportuno preservare il suo carattere neutro sotto il profilo tecnologico. Sono stati tuttavia rilevati problemi la cui risoluzione pone sfide specifiche. Si annoverano in particolare quelli che seguono.

- *Gestire l'impatto delle nuove tecnologie*

Dalle risposte di privati e organizzazioni fornite nel quadro delle consultazioni emerge la necessità di chiarire e precisare l'applicazione dei principi di protezione dei dati rispetto alle nuove tecnologie, al fine di garantire una protezione reale ed efficace dei dati a carattere personale, a prescindere dalle tecnologie usate per il trattamento, e risulta che i responsabili del trattamento sono pienamente consapevoli delle implicazioni delle nuove tecnologie per la protezione dei dati. Il problema è stato parzialmente affrontato con la direttiva 2002/58/CE ("direttiva relativa alla vita privata e alle comunicazioni elettroniche")[5] che specifica e integra la direttiva generale relativa alla protezione dei dati nel settore delle comunicazioni elettroniche[6].

---

3 Le risposte alla consultazione pubblica della Commissione figurano nel sito:http://ec.europa.eu/justice/news/events/events_en.htm. Nel 2010 si sono svolte consultazioni più mirate delle parti interessate e il 5 ottobre la vicepresidente della Commissione Viviane Reding ha presieduto una riunione di alto livello con le parti interessate a Bruxelles. La Commissione ha altresì consultato il Gruppo di lavoro articolo 29 che ha contribuito in misura esauriente alle consultazioni del 2009 (WP 168) e che, nel luglio 2010, ha adottato un parere sul principio di responsabilità (WP 173).

4 Oltre allo studio citato alla nota 2, si veda lo studio comparativo sui diversi approcci alle nuove sfide poste alla privacy (*Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*), gennaio 2010 http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). È in corso anche uno studio sulla valutazione d'impatto del nuovo quadro giuridico dell'UE sulla protezione dei dati personali.

5 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

6 La direttiva 95/46/CE sulla protezione dei dati definisce le norme per la protezione dei dati per tutti gli atti giuridici dell'UE, tra cui anche la direttiva 2002/58/EC relativa alla vita privata e alle comunicazioni elettroniche (modificata dalla direttiva 2009/136/CE, GU L 337 del 18.12.2009, pag. 11). La direttiva relativa alla vita privata e alle comunicazioni elettroniche si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione. Essa traduce i principi definiti nella direttiva sulla protezione dei dati in norme specifici per il settore delle comunicazioni elettroniche. La direttiva 95/46/CE si applica anche ai servizi di comunicazione non accessibili al pubblico.

- *Rafforzare la dimensione "mercato interno" della protezione dei dati*

Una delle preoccupazioni più frequenti delle parti interessate, in particolare delle società multinazionali, è l'insufficiente armonizzazione tra le norme di protezione dei dati degli Stati membri, e ciò nonostante l'esistenza di un quadro giuridico comune dell'Unione. Le parti hanno sottolineato la necessità di migliorare la certezza giuridica, ridurre gli oneri amministrativi e assicurare condizioni eque agli operatori economici e ad altri responsabili del trattamento.

- *Rispondere alla globalizzazione e migliorare il trasferimento internazionale dei dati*

Diverse parti interessate hanno evidenziato che il crescente ricorso all'outsourcing per il trattamento dei dati, molto spesso al di fuori dell'UE, pone diversi problemi in relazione al diritto applicabile al trattamento e all'attribuzione della responsabilità in merito. Per quanto riguarda il trasferimento internazionale di dati, molte organizzazioni ritengono che i regimi attuali non siano del tutto soddisfacenti e debbano essere rivisti e razionalizzati per semplificare i trasferimenti e renderli meno macchinosi.

- *Rafforzare l'assetto istituzionale per un'applicazione effettiva delle norme di protezione dei dati*

Le parti interessate concordano sulla necessità di rafforzare il ruolo delle autorità di protezione dei dati così da migliorare l'applicazione delle norme. Alcune organizzazioni sollecitano più trasparenza in relazione all'attività del Gruppo di lavoro articolo 29 (*si veda il punto 2.5*) e chiedono che ne vengano chiarite le funzioni e le competenze.

- *Migliorare la coerenza del quadro giuridico sulla protezione dei dati*

Nella consultazione pubblica, tutte le parti interessate hanno sottolineato la necessità di disporre di uno strumento globale applicabile al trattamento dei dati in tutti i settori e per tutte le politiche dell'Unione, capace di garantire un approccio integrato e una protezione senza soluzione di continuità, sistematica ed efficace[7].

Per far fronte a queste sfide **l'UE deve mettere a punto un approccio generale e coerente onde garantire che il diritto fondamentale di ciascuno alla protezione dei dati personali sia pienamente rispettato all'interno e all'esterno dell'UE**. Il trattato di Lisbona ha dotato l'Unione di ulteriori mezzi per raggiungere questo obiettivo: la Carta dei diritti fondamentali dell'Unione europea, il cui articolo 8 riconosce il diritto alla protezione dei dati personali, è divenuta giuridicamente vincolante ed è stata istituita una nuova base giuridica[8] che consente di stabilire norme dell'Unione sistematiche e coerenti di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla libera circolazione di tali dati. In particolare, la nuova base giuridica consente all'UE di disporre di un unico strumento giuridico per disciplinare la protezione dei dati, e ciò anche nei settori della cooperazione di polizia e della cooperazione giudiziaria in materia penale. L'ambito della politica estera e di sicurezza comune è solo parzialmente coperto dall'articolo 16 del TFUE, poiché a stabilire le

---

[7] In contributi separati presentati dopo la chiusura della consultazione pubblica, Europol ed Eurojust hanno comunque chiesto che si tenga conto della specificità del loro lavoro in relazione al coordinamento delle attività di contrasto e prevenzione della criminalità.

[8] Cfr. l'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE).

norme relative al trattamento dei dati da parte degli Stati membri deve essere una decisione del Consiglio che si fonda su un'altra base giuridica[9].

Sulla scorta di queste nuove possibilità, la Commissione darà priorità assoluta in tutte le sue politiche al rispetto del diritto fondamentale alla protezione dei dati in tutta l'Unione e rafforzerà contemporaneamente la dimensione "mercato interno", agevolando la libera circolazione dei dati personali. Nell'assicurare il diritto fondamentale alla protezione dei dati personali occorre però tener conto anche di altri importanti diritti fondamentali sanciti dalla Carta e di altri obiettivi previsti dai trattati.

Obiettivo della presente comunicazione è definire l'approccio della Commissione per modernizzare 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 in modo da continuare a garantire un elevato livello di protezione delle persone fisiche con riguardo al trattamento dei dati personali in quei settori. L'Unione europea continuerà così a svolgere un ruolo trainante nel promuovere norme elevate di protezione dei dati nel mondo intero.

2. OBIETTIVI CHIAVE DELL'APPROCCIO GLOBALE ALLA PROTEZIONE DEI DATI

2.1. Rafforzare i diritti delle persone

2.1.1. Garantire una protezione adeguata in ogni circostanza

Obiettivo delle norme fissate dagli attuali strumenti dell'UE per la protezione dei dati è **la tutela dei diritti fondamentali delle persone fisiche, in particolare del diritto alla protezione dei dati personali**, conformemente alla Carta dei diritti fondamentali dell'Unione europea[10].

Il concetto di "dati personali" è uno dei concetti essenziali per la tutela delle persone delle norme europee di protezione dei dati; da esso deriva l'applicazione degli obblighi che incombono ai responsabili del trattamento e agli incaricati del trattamento[11]. La definizione di "dati personali" intende coprire qualsiasi informazione concernente una persona fisica identificata o identificabile, direttamente o indirettamente. Per determinare se una persona è identificabile, è opportuno prendere in considerazione "l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona"[12]. Tale approccio è stato scelto deliberatamente dal legislatore per la sua flessibilità, in quanto applicabile a svariate situazioni e sviluppi concernenti i diritti fondamentali, compresi quelli che non erano prevedibili al momento dell'adozione della direttiva. Tuttavia, la conseguenza di un approccio tanto ampio e flessibile è che in molti casi, nell'applicare la direttiva, non è sempre chiaro come porsi: se dal punto di vista dell'interessato che gode del

---

9 Cfr. l'articolo 16, paragrafo 2, ultimo comma, del TFUE e l'articolo 39 del trattato sull'Unione europea.

10 Cfr. le cause C-101/01 *Bodil Lindqvist*, raccolta della giurisprudenza 2003 pagine I-1297, punti 96 e 97, e C-275/06 *Productores de Música de España (Promusicae)/Telefónica de España SAU*, raccolta della giurisprudenza 2008 pagina I-271. Cfr. anche la giurisprudenza della Corte europea dei diritti dell'uomo, ad es. le cause S. and **Marper**/United Kingdom del 4.12.2008 (domanda n. 30562/04 e 30566/04) e Rotaru /Romania del 4.5. 2000 (domanda n. 28341/95), paragrafo 55, ECHR 2000-V.

11 Cfr. la definizione di "responsabile del trattamento" e "incaricato del trattamento" di cui all'articolo 2, lettere d) ed e), della direttiva 95/46/CE.

12 Considerando 26 della direttiva 95/46/CE.

diritto alla protezione dei dati o da quello del responsabile del trattamento che deve sottostare agli obblighi imposti dalla direttiva[13].

Si verificano situazioni che implicano il trattamento di informazioni specifiche per le quali, in base al diritto dell'Unione, sarebbero necessarie ulteriori misure. In alcuni casi tali misure esistono. Ad esempio, stoccare dati in apparecchi terminali come i cellulari è permesso solo a condizione che l'interessato abbia dato il proprio consenso. Sarebbe opportuno esaminare la questione a livello dell'UE per quanto riguarda, ad esempio, i dati codificati con chiave, i dati relativi all'ubicazione, le tecnologie di *data mining* che combinano dati provenienti da fonti diverse, o i casi in cui vada assicurata la riservatezza e l'integrità dei sistemi informatici[14].

Tutti questi aspetti richiedono quindi un esame approfondito.

La Commissione valuterà **in che modo assicurare l'applicazione coerente delle norme di protezione dei dati, tenendo conto delle ripercussioni delle nuove tecnologie sui diritti e sulle libertà delle persone e dell'obiettivo di garantire la libera circolazione dei dati personali nel mercato interno.**

2.1.2. Migliorare la trasparenza per gli interessati

La trasparenza è una condizione fondamentale per permettere alle persone di esercitare un controllo sui propri dati e per assicurare una protezione efficace dei dati personali. È pertanto essenziale che gli interessati ricevano informazioni **corrette, chiare e trasparenti** dai responsabili del trattamento in merito alle modalità di raccolta e di trattamento dei dati che li riguardano, a chi li raccoglie e li tratta, per quali motivi e per quanto tempo, nonché al diritto di accesso ai dati, di rettifica e cancellazione. Le disposizioni relative alle informazioni da fornire all'interessato[15] non sono sufficienti.

Presupposti ineludibili della trasparenza sono **informazioni facilmente accessibili e comprensibili e l'uso di un linguaggio chiaro e semplice**. Ciò vale a maggior ragione per gli ambienti in rete, dove le informazioni riguardanti la privacy sono spesso poco chiare, difficilmente accessibili, non trasparenti[16] e non sempre del tutto conformi alle norme vigenti. Un esempio è la pubblicità comportamentale online, un campo in cui il forte aumento degli attori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia molto difficile per le persone comprendere se vengono raccolti dati personali, da chi e a quale scopo.

I **minori** devono essere particolarmente protetti al riguardo, in quanto sono probabilmente meno consapevoli dei rischi, delle conseguenze, delle garanzie e dei diritti inerenti al trattamento dei dati personali[17].

---

13 Cfr. ad esempio il caso degli indirizzi IP, esaminato dal Gruppo di lavoro articolo 29 nel parere 4/2007 sul concetto di dati personali (WP 136).

14 Cfr. ad esempio la sentenza della Corte costituzione federale tedesca (*Bundesverfassungsgericht*) del 27 febbraio 2008, 1 BvR 370/07.

15 Cfr. l'articolo 10 della direttiva 95/46/CE.

16 Un'indagine Eurobarometro condotta nel 2009 ha rilevato che circa la metà degli intervistati ritiene che nei siti web le informazioni relative alla privacy siano poco chiare o assolutamente poco chiare (cfr. Eurobarometro Flash n. 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf)

17 Cfr. lo studio qualitativo *Safer Internet for Children* (Internet più sicuro per i minori); lo studio, che ha interessato due fasce di età (9-10 e 12-14 anni), ha rilevato che i minori tendono a sottovalutare i rischi connessi all'uso di internet e a sminuire le conseguenze dei loro comportamenti a rischio (studio consultabile su:http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

La Commissione intende:

- integrare nel quadro giuridico un **principio generale di trasparenza del trattamento** dei dati personali;

- introdurre **obblighi specifici** a carico dei responsabili del trattamento in merito al tipo di informazioni da trasmettere e alle **modalità** per farlo, anche in relazione ai **minori**;

- elaborare uno o più **moduli standard UE** (**avvisi informativi sulla privacy**) ad uso dei responsabili del trattamento.

È inoltre importante che gli interessati sappiano se i loro dati sono andati distrutti, persi, sono stati alterati, consultati o comunicati a terzi non autorizzati, in modo accidentale o illegale. La recente revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche ha introdotto l'**obbligo di comunicare le violazioni di dati personali**, anche se solo per il settore delle telecomunicazioni. Dato che il rischio di violazione dei dati esiste anche in altri settori (ad esempio quello finanziario), la Commissione esaminerà le modalità per estendere tale obbligo di notifica anche ad altri settori, conformemente alla dichiarazione della Commissione sulla comunicazione della violazione dei dati fatta davanti al Parlamento europeo nel 2009 nell'ambito della riforma del quadro normativo per le comunicazioni elettroniche[18]. Tale esame non riguarderà le disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche che deve essere recepita negli ordinamenti nazionali entro il 25 maggio 2011[19]. Occorre garantire un approccio sistematico e coerente alla questione.

La Commissione intende:

- esaminare le modalità per integrare nel quadro giuridico generale un **obbligo generale di comunicare le violazioni di dati personali**, che specifichi i destinatari della notifica e i criteri per l'applicazione di tale obbligo.

2.1.3. Rafforzare il controllo dei propri dati

Due premesse importanti per garantire un elevato livello di protezione dei dati sono che il **trattamento dati effettuato dal responsabile sia limitato al minimo necessario in relazione alle sue finalità (principio di minimizzazione dei dati)** e che l'interessato mantenga un **controllo effettivo dei propri dati**. L'articolo 8, paragrafo 2, della Carta recita: "Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica". Chiunque dovrebbe essere sempre in grado di accedere ai propri dati, rettificarli, cancellarli o bloccarli, a meno che motivi legittimi previsti dalla legge non vi si oppongano. Tali diritti sono già integrati nel quadro giuridico vigente, eppure il modo in cui possono

---

18 "La Commissione prende atto della volontà del Parlamento europeo che l'obbligo di comunicazione delle violazioni dei dati personali non sia limitato al settore delle comunicazioni elettroniche, ma si applichi anche a soggetti come i fornitori di servizi della società dell'informazione [...]. Pertanto, la Commissione avvierà senza indugio il lavoro preparatorio adeguato, ivi compresa la consultazione con le parti interessate, allo scopo di presentare, se del caso, proposte in questo settore entro il 2011[…]", consultabile sul sito: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//IT. Cfr. anche il considerando 59 della direttiva 2009/136/CE che modifica la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche: "L'interesse generale degli utenti a essere informati non si limita ovviamente al settore delle comunicazioni elettroniche e, conseguentemente, l'introduzione a livello comunitario di prescrizioni esplicite e obbligatorie relative alla comunicazione delle violazioni dovrebbe ricevere carattere prioritario."

19 Cfr. l'articolo 4 della direttiva 2009/136/CE.

essere esercitati non è armonizzato e, di fatto, in alcuni Stati membri sono tutelati meglio che in altri. La questione diventa scottante negli ambienti online, dove i dati sono spesso conservati senza che l'interessato lo sappia e/o abbia dato il consenso.

Particolarmente rilevante al riguardo è l'esempio dei siti di social network, che oppongono grandi difficoltà a chi voglia esercitare un controllo effettivo dei propri dati personali. La Commissione ha ricevuto varie denunce di persone che non sono riuscite a recuperare dati personali, anche fotografie, da fornitori di servizi online e che quindi non hanno potuto esercitare i diritti di accesso, rettifica e cancellazione.

Sarebbe opportuno rendere tali diritti più espliciti e chiari, e possibilmente rafforzarli.

La Commissione esaminerà quindi i mezzi per:

- rafforzare il **principio di minimizzazione dei dati**;

- **migliorare le modalità** per l'effettivo **esercizio dei diritti di accesso, rettifica e cancellazione o blocco dei dati** (ad esempio introducendo termini di risposta alle richieste degli interessati, consentendo l'esercizio dei diritti per via elettronica o stabilendo che il diritto di accesso debba essere di norma gratuito);

- chiarire il cosiddetto "**diritto all'oblio"**, ossia il diritto di far cessare il trattamento dei propri dati e di farli cancellare quando non sono più necessari per fini legittimi. È quanto accade, ad esempio, quando il trattamento è basato sul consenso dell'interessato e questi lo ritira, oppure alla scadenza del periodo di conservazione;

- integrare i diritti degli interessati assicurando il diritto di "**data portability**", ovvero il diritto esplicito di cancellare i propri dati (ad esempio foto, cartelle mediche o elenchi di amici) da un'applicazione o un servizio e, se tecnicamente possibile, di trasferirli a un'altra applicazione o servizio, senza opposizione del responsabile del trattamento.

2.1.4. Sensibilizzare

La trasparenza è certamente un elemento essenziale, ma occorre anche sensibilizzare di più il grande pubblico, in particolare i giovani, sui rischi riguardanti il trattamento dei dati personali e sui diritti dell'interessato. Un'indagine Eurobarometro del 2008 ha rivelato che la maggior parte dei cittadini dell'Unione ritiene che vi sia scarsa consapevolezza della protezione dei dati personali nel proprio paese[20]. Le iniziative di sensibilizzazione dovrebbero essere incoraggiate e promosse da più parti: dalle amministrazioni degli Stati membri, in particolare dalle autorità di protezione dei dati e dagli organi preposti all'istruzione, dai responsabili dei dati e dalle associazioni della società civile, e dovrebbero comprendere misure non legislative, come le campagne di sensibilizzazione nella stampa e nei media elettronici, informazioni chiare sui siti web e chiare specificazioni dei diritti dell'interessato e degli obblighi del responsabile del trattamento.

[20] Cfr. Eurobarometro Flash n. 225 – Protezione dei dati nell'Unione europea: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

La Commissione esaminerà:

-la possibilità di **cofinanziare,** tramite il bilancio dell'Unione, **attività di sensibilizzazione in merito alla protezione dei dati**;

- la necessità e l'opportunità di integrare nel quadro giuridico **l'obbligo di svolgere attività di sensibilizzazione** in questo settore.

2.1.5. Garantire un consenso libero e informato

Laddove è necessario il consenso informato, le norme vigenti prevedono che il consenso dell'interessato al trattamento dei dati personali che lo riguardano debba tradursi in una "manifestazione di volontà libera, specifica e informata" con la quale l'interessato segnala di essere d'accordo con il trattamento[21]. Tuttavia dette condizioni sono al momento interpretate in modo diverso nei diversi Stati membri; così, ad esempio, mentre in alcuni Stati vige l'obbligo generale del consenso scritto, altri presuppongono il tacito consenso.

Inoltre, negli ambienti online - data l'opacità delle politiche relative alla privacy - è spesso ancora più difficile comprendere i propri diritti e dare un consenso informato. Ciò è ulteriormente complicato dal fatto che talvolta non è nemmeno chiaro in che cosa consista il consenso libero, specifico e informato; è questo il caso della pubblicità comportamentale, dove le impostazioni del browser esprimono, secondo alcuni ma non secondo tutti, il consenso dell'utente.

È quindi opportuno fare chiarezza sulle condizioni per il consenso, onde garantire che questo sia dato sempre con conoscenza di causa e che l'interessato ne sia pienamente consapevole e sappia per quale trattamento lo sta accordando, come prevede l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. Disposizioni essenziali chiare possono inoltre favorire lo sviluppo di iniziative di autoregolamentazione e la ricerca di soluzioni pratiche conformi al diritto dell'UE.

La Commissione esaminerà come **rendere più chiare e rafforzare le norme sul consenso**.

2.1.6. Proteggere i dati sensibili

Il trattamento dei dati sensibili, di quei dati cioè che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'appartenenza sindacale, e il trattamento di dati relativi alla salute e alla vita sessuale sono già vietati in linea generale, salvo limitate eccezioni quando ricorrono determinate condizioni e garanzie[22]. I mutamenti tecnologici e sociali impongono tuttavia di riesaminare le disposizioni vigenti in materia di dati sensibili per valutare se sia necessario aggiungere altre categorie di dati e specificare le condizioni del trattamento. Ciò vale, per esempio, per i dati genetici che non sono al momento esplicitamente considerati dati sensibili.

[21] Cfr. articolo 2, lettera h), della direttiva 95/46/CE.

[22] Cfr. articolo 8 della direttiva 95/46/CE.

La Commissione intende esaminare:

- se vi sono altre categorie di dati che debbano essere considerate "**dati sensibili**", ad esempio i dati **genetici**;

- specificare ulteriormente e **armonizzazione le condizioni** per il trattamento delle categorie di dati sensibili.

2.1.7. Rendere più efficaci i mezzi di ricorso e le sanzioni

Onde assicurare l'attuazione delle norme di protezione dei dati, occorre assolutamente una **normativa efficace in materia di mezzi di ricorso e sanzioni**. La violazione del diritto alla protezione dei dati personali di una singola persona riguarda in molti casi anche molte altre persone che si trovano in una situazione simile.

Per questo la Commissione intende:

- considerare la possibilità di **ampliare le competenze** delle autorità di protezione dei dati, delle associazioni della società civile e di **altre associazioni che rappresentano gli interessi dei soggetti cui si riferiscono i dati** per **avviare un'azione legale dinanzi al giudice nazionale**;

- valutare la necessità di **rafforzare le disposizioni esistenti in materia di sanzioni**, ad esempio includendo esplicitamente sanzioni penali nel caso di violazione grave delle norme di protezione dei dati, al fine di renderle più efficaci.

2.2. Rafforzare la dimensione "mercato interno"

2.2.1. Accrescere la certezza giuridica e assicurare condizioni eque ai responsabili del trattamento

La protezione dei dati nell'UE 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. L'armonizzazione delle legislazioni nazionali tramite la direttiva non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa[23].

Al contempo la direttiva riconosce agli Stati membri un margine di manovra in taluni settori e li autorizza a mantenere o a istituire regimi particolari per situazioni specifiche[24]. Questo e il fatto che in alcuni casi la direttiva non è stata correttamente attuata dagli Stati membri hanno alimentato **divergenze tra le leggi nazionali di attuazione della direttiva che ostacolano uno degli obiettivi principali della direttiva stessa, ossia la libera circolazione dei dati personali nel mercato interno**. Ciò vale per un gran numero di settori e di ambiti, ad esempio per il trattamento dei dati personali sul lavoro o per motivi di salute pubblica. La mancata armonizzazione è in effetti uno dei principali problemi ricorrenti segnalati dalle parti interessate del settore privato, soprattutto dagli operatori economici, in quanto comporta costi supplementari e oneri amministrativi. Particolarmente problematica è la situazione dei responsabili del trattamento stabiliti in più Stati membri, di cui devono rispettare le disposizioni e le prassi vigenti. Inoltre, le differenze nell'attuazione della direttiva negli Stati

[23] Cfr. la causa C-1001/01 *Bodil Lindqvist*, raccolta della giurisprudenza 2003 pagine I-1297, punti 96 e 97.

[24] *Ibidem*, punto 97. Cfr. anche il considerando 9 della direttiva 95/46/CE.

membri creano incertezza giuridica non solo ai responsabili del trattamento, ma anche agli interessati, rischiando di compromettere quel livello equivalente di protezione che la direttiva dovrebbe instaurare e garantire.

La Commissione esaminerà i mezzi per conseguire **una maggiore armonizzazione delle norme di protezione dei dati a livello dell'UE**.

2.2.2. Ridurre gli oneri amministrativi

Garantire condizioni eque significa che vi sarà meno necessità di ottemperare a disposizioni nazionali divergenti, riducendo quindi drasticamente gli oneri amministrativi a carico dei responsabili del trattamento. La **revisione e la semplificazione dell'attuale sistema di notificazione**[25] contribuirebbe concretamente a diminuire gli oneri amministrativi e ridurre i costi dei responsabili del trattamento. I responsabili del trattamento concordano in generale che l'attuale obbligo di notificare tutti i trattamenti dati alle autorità di protezione dei dati sia alquanto gravoso e di per sé non aggiunga molto alla protezione dei dati personali. Inoltre, questo è uno dei punti in cui la direttiva lascia un certo margine di manovra agli Stati membri, che sono liberi di decidere in merito a possibili esenzioni o semplificazioni e di scegliere le procedure da applicare.

Un **sistema armonizzato e semplificato** ridurrebbe i costi e gli oneri amministrativi, soprattutto per le società multinazionali stabilite in più Stati membri.

La Commissione esaminerà diversi modi per **semplificare e armonizzare l'attuale sistema di notificazione**, compresa l'eventualità di introdurre un **modulo di registrazione uniforme per tutta l'UE**.

2.2.3. Chiarire le norme relative al diritto applicabile e alle competenze degli Stati membri

La prima relazione[26] della Commissione sull'applicazione della direttiva sulla protezione dei dati già nel 2003 evidenziava che l'applicazione della disposizione sul diritto applicabile[27] "in molti casi è lacunosa, con la conseguenza che potrebbero insorgere tra le legislazioni conflitti di quel tipo che l'articolo intendeva evitare." Da allora la situazione non è migliorata. Di conseguenza i responsabili del trattamento e le autorità di protezione dei dati non sempre sanno qual è lo Stato membro competente e quale il diritto applicabile quando più Stati membri sono coinvolti. Ciò vale soprattutto se il responsabile del trattamento deve rispettare disposizioni differenti di diversi Stati membri, se una multinazionale è stabilita in più Stati membri o se il responsabile del trattamento non è stabilito nell'UE ma fornisce servizi a persone residenti nell'UE.

Anche la globalizzazione e lo sviluppo tecnologico creano complessità: è sempre più frequente il caso di responsabili del trattamento che operano in diversi Stati membri, sottostando così a più giurisdizioni, e che forniscono servizi e assistenza 24 ore su 24. Grazie a internet, i responsabili del trattamento stabiliti al di fuori dello spazio economico europeo (SEE)[28] possono fornire con maggior facilità servizi a distanza e trattare dati personali in

---

25 Cfr. l'articolo 18 della direttiva 95/46/CE.

26 Relazione della Commissione - Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) (COM (2003) 265 definitivo).

27 Cfr. l'articolo 4 della direttiva 95/46/CE.

28 Lo spazio economico europeo comprende la Norvegia, il Liechtenstein e l'Islanda.

ambienti online; inoltre, è spesso difficile localizzare i dati personali e le apparecchiature usate di volta in volta (ad esempio nelle applicazioni e nei servizi di cloud computing).

Tuttavia, secondo la Commissione il fatto che i dati personali siano trattati da responsabili stabiliti in un paese terzo non deve privare le persone della protezione cui hanno diritto a norma della Carta dei diritti fondamentali dell'Unione europea e delle norme di protezione dei dati dell'UE.

La Commissione esaminerà le modalità per **rivedere e chiarire le disposizioni vigenti in materia di diritto applicabile**, compresi gli attuali criteri determinanti, al fine di migliorare la certezza giuridica, di chiarire le competenze degli Stati membri nell'applicare le norme di protezione dei dati e di garantire lo stesso livello di protezione alle persone residenti nell'UE, a prescindere dalla localizzazione geografica dal responsabile del trattamento.

2.2.4. Ampliare gli obblighi del responsabile del trattamento

La semplificazione amministrativa **non deve comportare una riduzione generale degli obblighi a carico dei responsabili del trattamento per una protezione efficace dei dati**. La Commissione ritiene, al contrario, che il nuovo quadro giuridico debba definire più chiaramente tali obblighi, anche in relazione ai dispositivi di controllo interno e alla cooperazione con le autorità nazionali di protezione dei dati. Questa responsabilità dovrà poi applicarsi anche a quei responsabili del trattamento che sottostanno al segreto professionale (ad esempio i legali) nonché in tutti i casi, sempre più frequenti, in cui i responsabili delegano il trattamento a terzi (ad esempio agli incaricati).

La Commissione studierà i mezzi per **garantire che i responsabili del trattamento mettano in atto politiche e meccanismi efficaci al fine di assicurare il rispetto delle norme di protezione dei dati**. Al riguardo terrà conto del dibattito in corso sull'introduzione del principio di "accountability"[29]. L'obiettivo non sarà aumentare gli oneri amministrativi per i responsabili del trattamento, poiché tali misure intendono piuttosto instaurare garanzie e meccanismi di protezione più efficaci, riducendo e semplificando alcune formalità amministrative quali la notificazione (*si veda il punto 2.2.2*).

Potrebbe rivelarsi importante a questo proposito promuovere l'uso delle tecnologie di rafforzamento della tutela della vita privata (PET - Privacy Enhancing Technologies), come già evidenziato dalla comunicazione della Commissione del 2007 sull'argomento, e del principio "privacy by design", anche per garantire la sicurezza dei dati[30].

29 Cfr. il parere adottato dal Gruppo articolo 29 il 13 luglio, 3/2010.

30 Cfr. la comunicazione della Commissione al Parlamento europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET – Privacy Enhancing Technologies), COM(2007) 228. In base al principio della "privacy by design" la protezione della vita privata e dei dati personali è integrata in tutto il ciclo di vita delle tecnologie, dalla fase di progettazione iniziale allo sviluppo, uso e smaltimento finale. Questo principio figura tra l'altro nella comunicazione della Commissione "Un'agenda digitale europea", COM(2010) 245.

La Commissione prenderà in esame le seguenti misure per rafforzare gli obblighi a carico dei responsabili del trattamento:

– rendere obbligatoria la nomina di un **responsabile della protezione dei dati** indipendente e armonizzare le regole sulle sue funzioni e competenze[31], riflettendo però ad una soglia adeguata per evitare di gravare soprattutto le piccole imprese e le microimprese di inutili oneri amministrativi;

– integrare nel quadro giuridico l'obbligo per i responsabili del trattamento di realizzare in casi specifici una **valutazione d'impatto della protezione dei dati**, ad esempio per il trattamento di dati sensibili o se il tipo di trattamento presenta rischi particolari, soprattutto in connessione con determinate tecnologie, procedure e dispositivi, tra cui la profilazione o la videosorveglianza;

– promuovere l'uso delle PET e le possibilità di attuazione concreta del concetto "**privacy by design**".

2.2.5. Incoraggiare le iniziative di autoregolamentazione ed esplorare regimi di certificazione dell'UE

La Commissione continua a ritenere che le **iniziative di autoregolamentazione** dei responsabili del trattamento possano **contribuire a migliorare l'applicazione delle norme di protezione dei dati**. Finora sono state raramente applicate le disposizioni della direttiva sulla protezione dei dati relative all'autoregolamentazione, ovvero all'elaborazione di codici di condotta[32], ritenute insoddisfacenti dalle parti interessate.

La Commissione esaminerà inoltre l'eventualità di creare **regimi europei di certificazione** (ad esempio **marchi di certificazione** o privacy seals) per procedimenti, tecnologie, prodotti e servizi "ottemperanti ai principi di tutela della vita privata"[33]. Ciò servirebbe non solo ad orientare le persone che usano tali tecnologie, prodotti e servizi, ma sarebbe utile anche in relazione agli obblighi del responsabile del trattamento: scegliendo tecnologie, prodotti o servizi certificati, questi potrebbe dimostrare di avervi ottemperato (*si veda il punto 2.2.3*). Naturalmente **l'attendibilità di tali marchi di certificazione dovrebbe essere assolutamente garantita**, così come la loro conformità con gli obblighi legali e gli standard tecnici internazionali.

La Commissione intende:

- esaminare le possibilità di **incoraggiare ulteriormente le iniziative di autoregolamentazione**, tra cui la promozione attiva dei codici di condotta;

- studiare la fattibilità di **regimi europei di certificazione** nel campo della tutela della vita privata e dei dati personali.

---

31 La possibilità attuale che un responsabile del trattamento nomini un responsabile della protezione dei dati affinché garantisca in modo indipendente il rispetto delle norme di protezione dei dati nazionali e dell'UE e assista gli interessati si riscontra in diversi Stati membri (si pensi al "*Beauftragter für den Datenschutz*" in Gemania e al "*correspondant informatique et libertés* (CIL)" in Francia).

32 Cfr. l'articolo 27 della direttiva 95/46/CE.

33 Cfr. anche la comunicazione sulle PET citata alla nota 30.

2.3. Rivedere le norme di protezione dei dati nell'ambito della cooperazione di polizia e giudiziaria in materia penale

La direttiva sulla protezione dei dati si applica a tutte le attività di trattamento dei dati personali negli Stati membri, sia nel settore pubblico che in quello privato. Non si applica invece ai trattamenti di dati personali "effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario" quali le attività nei settori della cooperazione di polizia e giudiziaria in materia penale[34]. Il trattato di Lisbona ha tuttavia abolito la precedente "struttura a pilastri" dell'UE e ha creato una nuova base giuridica generale per la protezione dei dati personali in tutte le politiche dell'Unione[35]. Con queste premesse e vista la Carta dei diritti fondamentali dell'Unione europea, le comunicazioni della Commissione relative al programma di Stoccolma e al piano d'azione per l'attuazione del programma di Stoccolma[36] hanno evidenziato la necessità di istituire un "regime completo di protezione" e "rafforzare la posizione dell'UE in relazione alla protezione dei dati personali in tutte le politiche europee, anche nel contrastare e prevenire la criminalità".

Lo strumento dell'UE che disciplina la protezione dei dati personali nei settori della cooperazione di polizia e giudiziaria in materia penale è la **decisione quadro 2008/977/GAI**[37]. La decisione quadro è un importante passo avanti in un campo in cui vi era assoluta necessità di norme comuni in materia di protezione dei dati, ma resta ancora molto da fare.

La decisione quadro si applica solo agli scambi transfrontalieri di dati personali all'interno dell'UE, ma non ai trattamenti di dati all'interno degli Stati membri. Nella prassi è difficile separare questi due processi e ciò può complicare l'attuazione e l'applicazione effettiva della decisione quadro[38].

Di conseguenza, **la decisione quadro prefigura un'eccezione troppo ampia al principio di limitazione delle finalità**. Mancano inoltre disposizioni per distinguere diverse categorie di dati in base al loro grado di esattezza e affidabilità; così i dati fondati su fatti dovrebbero essere differenziati da quelli fondati su opinioni o valutazioni personali[39] e si dovrebbe anche distinguere tra le diverse categorie di persone interessate (autori di reato, indiziati, vittime, testimoni, ecc.), fornendo garanzie specifiche per i dati relativi a persone non sospette[40].

Per giunta, **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**

---

34 Cfr. l'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46/CE.

35 Cfr. l'articolo 16 del TFUE.

36 Cfr. COM(2009) 262 del 10.6.2009 e COM(2010) 171 del 20.4.2010.

37 Decisione quadro 2008/977/GAI del Consiglio, del 27.11.2008, 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). La decisione quadro persegue solo un livello minimo di armonizzazione delle norme di protezione dei dati.

38 Tale distinzione non viene operata nei pertinenti strumenti del Consiglio d'Europa, quali la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) e relativo protocollo addizionale concernente le autorità di controllo e i flussi transfrontalieri (STCE n. 181); la raccomandazione R (87) 15 del comitato dei Ministri del Consiglio d'Europa tesa a regolamentare l'utilizzo dei dati a carattere personale nel settore della polizia, adottata il 17 settembre 1987.

39 Come previsto dal principio 3.2 della raccomandazione R (87) 15.

40 Contrariamente al principio 2 della raccomandazione R (87) 15 e alle relative relazioni di valutazione.

materia penale[41], in particolare a quelli che disciplinano il funzionamento di Europol, Eurojust, il sistema d'informazione Schengen (SIS) e il sistema informativo doganale (SID)[42], 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. Per le attività relative alla cooperazione di polizia e giudiziaria tutti gli Stati membri hanno sottoscritto la raccomandazione R (87) 15 del Consiglio d'Europa, che definisce i principi della convenzione 108 per il settore della polizia. Tuttavia, la raccomandazione non è uno strumento giuridicamente vincolante.

Tale stato di cose può avere conseguenze dirette sulla possibilità delle persone di esercitare i propri diritti alla protezione dei dati che li riguardano in questo settore (ad esempio il diritto di sapere quali dati sono trattati e scambiati, chi compie tali operazioni e per quale fine, come esercitare diritti come il diritto di accesso ai propri dati).

Se l'obiettivo è istituire un sistema coerente e globale nell'UE e nei confronti dei paesi terzi, **occorre allora contemplare una revisione delle norme vigenti di protezione dei dati nel settore della cooperazione di polizia e giudiziaria in materia penale**. La Commissione sottolinea che la nozione di regime completo di protezione dei dati non esclude che nel quadro generale siano previste norme specifiche di protezione dei dati per i settori di polizia e giudiziario, in considerazione della loro specificità, come indicato nella dichiarazione 21 allegata al trattato di Lisbona. Ciò significa, ad esempio, che occorre esaminare in quale misura l'esercizio di alcuni diritti riguardanti la protezione dei dati rischi, in casi specifici, di compromettere la prevenzione, l'indagine, l'accertamento di reati e l'azione penale o finanche l'esecuzione di sanzioni penali.

In particolare, la Commissione intende:

- valutare se **estendere l'applicazione delle norme generali di protezione dei dati ai settori della cooperazione di polizia e giudiziaria in materia penale**, anche per il trattamento a livello nazionale, prevedendo se del caso **limitazioni armonizzate** di alcuni diritti riguardanti la protezione dei dati, ad esempio il diritto di accesso o il principio di trasparenza;

- esaminare se il nuovo quadro giuridico generale sulla protezione dei dati debba contenere **disposizioni specifiche e armonizzate**, riguardanti ad esempio il trattamento dei **dati genetici** a fini penali o la distinzione tra le diverse categorie di persone interessate (testimoni, indiziati, ecc.) nel settore della cooperazione di polizia e giudiziaria in materia penale;

- avviare nel 2011 una **consultazione** di tutte le parti interessate sul metodo migliore per **revisionare gli attuali sistemi di controllo nei settori della cooperazione di polizia e giudiziaria in materia penale**, al fine di garantire un controllo reale e coerente della protezione dei dati in tutte le istituzioni, organi, organismi e agenzie dell'Unione;

- valutare la necessità di **allineare**, a lungo termine, **le numerose norme settoriali vigenti adottate a livello dell'UE per la cooperazione di polizia e giudiziaria in materia penale nell'ambito di strumenti specifici,** al nuovo quadro giuridico generale sulla protezione dei dati .

---

41 Tali strumenti sono passati in rassegna nella comunicazione della Commissione "Panorama generale della gestione delle informazioni nello spazio di libertà sicurezza e giustizia", COM (2010) 385.

42 Per assicurare il controllo della protezione dei dati sono state istituite autorità comuni di protezione dei dati sulla base degli strumenti pertinenti. Inoltre, ai sensi del regolamento (CE) n. 45/2001, il Garante europeo della protezione dei dati dispone di poteri di controllo generali sulle istituzioni, organi, organismi e agenzie dell'Unione.

2.4. La dimensione globale della protezione dei dati

2.4.1. Chiarire e semplificare le norme applicabili ai trasferimenti internazionali di dati

Il trasferimento di dati personali al di fuori dell'UE e del SEE è subordinato in particolare alla cosiddetta **"valutazione dell'adeguatezza"**, alla valutazione cioè della capacità di un paese terzo di garantire un livello di protezione adeguato ai sensi delle norme UE, cui attualmente possono provvedere la Commissione e gli Stati membri.

Se è la Commissione ad accertare l'adeguatezza, i dati possono circolare liberamente dai 27 Stati membri UE e dai tre paesi SEE verso il paese terzo interessato senza bisogno di ulteriori garanzie. Tuttavia, la direttiva sulla protezione dei dati non specifica i requisiti esatti affinché la Commissione riconosca l'adeguatezza, né la richiamata decisione quadro prevede che la Commissione prenda decisioni di questo tipo.

In alcuni Stati membri l'adeguatezza è valutata anzitutto dal responsabile del trattamento che opera il trasferimento dei dati verso un paese terzo, talvolta sotto il controllo ex-post dell'autorità di protezione dei dati. È quindi possibile che vengano utilizzati metodi diversi per valutare il livello di adeguatezza dei paesi terzi o delle organizzazioni internazionali con il **conseguente rischio che il livello di protezione dei dati offerto all'interessato in un paese terzo venga giudicato in modo diverso a seconda degli Stati membri**. Per giunta, gli attuali strumenti giuridici non prevedono requisiti armonizzati e precisi in base ai quali considerare un trasferimento legittimo. Tutto ciò si traduce in prassi che variano da uno Stato membro all'altro.

Nel caso di trasferimenti di dati a paesi terzi che non garantiscono un livello di protezione adeguato, le attuali clausole tipo della Commissione per il trasferimento di dati personali ai responsabili[43] e agli incaricati[44] del trattamento non sono concepite per situazioni extracontrattuali e, per esempio, non possono applicarsi al trasferimento di dati tra le pubbliche amministrazioni.

Inoltre gli accordi internazionali conclusi dall'UE o dai suoi Stati membri impongono spesso l'inserimento di principi di protezione dei dati e disposizioni specifiche, il che può tradursi in testi differenti contenenti disposizioni e diritti incompatibili tra loro e che danno adito ad interpretazioni divergenti a scapito dell'interessato. Per questo la Commissione ha annunciato che intende elaborare gli elementi essenziali di protezione dei dati personali degli accordi a fini di contrasto tra l'Unione e i paesi terzi[45].

Altri metodi messi a punto nell'ambito dell'autoregolamentazione, come i codici di condotta interni delle società, le cosiddette "norme vincolanti d'impresa" (*Binding Corporate Rules* -

---

43 Decisione della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE (GU L 181 del 4.7.2001, pag. 19); decisione della Commissione, del 27 dicembre 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE (GU L 6 del 10/01/2002, pag. 52); decisione della Commissione, del 27 dicembre 2004, che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi (GU L 385 del 29.12.2004, pag. 74).

44 Decisione della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio (GU L 39 del 12.02.2010, pag. 5);

45 Piano d'azione per l'attuazione del programma di Stoccolma (cfr. nota 36 supra).

BCR)[46], possono rivelarsi utili strumenti per trasferire legittimamente i dati personali tra società dello stesso gruppo. Le parti interessate hanno tuttavia segnalato che questo meccanismo potrebbe essere migliorato e la sua applicazione semplificata.

Per risolvere i problemi individuati sopra, **occorre migliorare in generale gli attuali meccanismi di trasferimento internazionale di dati personali**, garantendo nel contempo un'adeguata protezione dei dati personali trasferiti e trattati al di fuori dell'UE e del SEE.

La Commissione intende valutare le possibilità di:

- **migliorare e semplificare le attuali procedure** per i trasferimenti internazionali di dati, compresi gli strumenti giuridicamente vincolanti e le "norme vincolanti d'impresa", al fine di assicurare un **approccio dell'UE più uniforme e coerente** nei confronti dei paesi terzi e delle organizzazioni internazionali;

- **chiarire la propria procedura di valutazione dell'adeguatezza** e specificare meglio i **criteri e i requisiti** per valutare il livello di protezione dei dati offerto da un paese terzo o da un'organizzazione internazionale;

- definire gli **elementi essenziali di protezione dei dati** che potrebbero figurare in tutti i tipi di accordi internazionali.

2.4.2. Promuovere principi universali

Essendo un'operazione globalizzata il trattamento dei dati esige che si mettano a punto principi universali di tutela delle persone con riguardo al trattamento dei dati di carattere personale.

Il quadro giuridico dell'UE funge spesso da **punto di riferimento per paesi terzi nel regolamentare la protezione dei dati**. Il suo impatto e i suoi effetti all'interno e all'esterno dell'Unione, sono della massima importanza. **L'Unione europea deve pertanto rimanere una forza trainante per lo sviluppo e la promozione di norme internazionali di protezione dei dati personali, sia giuridiche che tecniche**, in conformità con gli strumenti pertinenti dell'UE e degli Stati membri in materia di protezione dei dati. Ciò è particolarmente importante nel contesto della politica di allargamento dell'UE.

Per quanto riguarda le norme tecniche internazionali messe a punto dagli organismi di normazione, la Commissione ritiene particolarmente importante che il futuro quadro giuridico sia conforme a tali norme, onde garantire un'attuazione pratica coerente delle norme di protezione dei dati da parte dei responsabili del trattamento.

[46] Le "norme vincolanti d'impresa" sono codici di pratiche che si basano sulle norme europee di protezione dei dati, stilati da organizzazioni multinazionali che li adottano su base volontaria per garantire un livello adeguato di protezione dei dati personali trasferiti tra imprese che, appartenendo a uno stesso gruppo, sono tenute a rispettare tali norme societarie. Cfr.: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

La Commissione intende:

- continuare a **promuovere lo sviluppo di elevate norme di protezione dei dati, sia tecniche che giuridiche,** nei paesi terzi e a livello internazionale;

- impegnarsi a favore del **principio della reciprocità della protezione** nelle azioni internazionali dell'Unione e soprattutto nei confronti delle persone i cui dati sono esportati dall'UE verso paesi terzi;

- **rafforzare a tal fine la cooperazione con i paesi terzi e le organizzazioni internazionali** come l'OCSE, il Consiglio d'Europa, le Nazioni Unite e altre organizzazioni regionali;

- **seguire da vicino lo sviluppo delle norme tecniche internazionali messe a punto dagli organismi di normazione** come il CEN e l'ISO, per sincerarsi che integrino proficuamente le norme giuridiche e assicurino il rispetto effettivo sul piano operativo dei requisiti fondamentali di protezione dei dati.

2.5. Rafforzare l'assetto istituzionale per un'applicazione effettiva delle norme di protezione dei dati

L'attuazione e l'applicazione dei principi e delle norme di protezione dei dati sono fondamentali per garantire il rispetto dei diritti delle persone.

In questo contesto, **il ruolo delle autorità di protezione dei dati è essenziale** per l'applicazione delle norme in materia. Esse sono i garanti indipendenti dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati di carattere personale. Per questo la Commissione crede che il loro ruolo vada rafforzato, vista in particolare la recente sentenza della Corte di giustizia europea sulla loro indipendenza[47], e che dovrebbero godere dei poteri e delle risorse necessarie per esercitare adeguatamente le loro funzioni, sia nel proprio Stato membro che cooperando con altre autorità.

Allo stesso tempo la Commissione ritiene che le **autorità di protezione dei dati debbano cooperare più strettamente e coordinare meglio le loro attività**, in particolare quando trattano questioni che, per loro natura, hanno una dimensione transfrontaliera. Questo vale soprattutto nel caso di società multinazionali stabilite in diversi Stati membri e attive in ciascuno di essi, o quando è richiesto un controllo coordinato con il Garante europeo della protezione dei dati[48].

Un ruolo importante in merito **può essere svolto dal Gruppo di lavoro articolo 29**[49] che, oltre a espletare funzioni consultive[50], deve anche contribuire all'applicazione uniforme negli Stati membri delle norme europee di protezione dei dati. Tuttavia, poiché le autorità di protezione dei dati continuano ad applicare e ad interpretare in modo diverso le norme UE anche quando le problematiche relative alla protezione dei dati sono le stesse in tutta l'UE,

---

47 Cfr. la sentenza 9 marzo 2010, causa C-518/07, *Commissione/Germania*.

48 È questo il caso dei sistemi TI su larga scala, come per esempio il SIS II (cfr. l'articolo 46 del regolamento (CE) n. 1987/2006 – GU L 318 del 28.12.2006, pag. 4) e il VIS (cfr. l'articolo 43 del regolamento (CE) n. 767/2008 – GU L 218 del 13.8.2008, pag. 60).

49 Il Gruppo di lavoro articolo 29 è un organo consultivo composto da un rappresentante delle autorità di protezione dei dati per ciascuno Stato membro, dal Garante europeo della protezione dei dati e dalla Commissione (che non ha diritto di voto) che espleta anche funzioni di segreteria. Cfr.: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 È compito del Gruppo di lavoro articolo 29 consigliare la Commissione sul livello di protezione nell'UE e nei paesi terzi e in merito a qualsiasi altra misura riguardante il trattamento dei dati personali.

occorre rafforzare il ruolo del Gruppo di lavoro in ordine al coordinamento delle posizioni delle autorità di protezione dei dati, in modo da assicurare un'applicazione più uniforme a livello nazionale e, quindi, un livello di protezione dei dati equivalente.

La Commissione intende esaminare:

- come **rafforzare, chiarire e armonizzare lo status e i poteri delle autorità nazionali di protezione dei dati** nel nuovo quadro giuridico, inclusa la piena attuazione del concetto di "piena indipendenza"[51];

- come **migliorare la cooperazione e il coordinamento tra le autorità di protezione dei dati;**

- come assicurare un'applicazione più coerente delle norme europee di protezione dei dati nel mercato interno, mediante, per esempio, il **rafforzamento del ruolo delle autorità nazionali di protezione dei dati, un miglior coordinamento delle loro attività attraverso il Gruppo di lavoro articolo 29 (che dovrebbe divenire un organo più trasparente) e/o la creazione di un meccanismo per la coerenza nel mercato interno, posto sotto l'autorità della Commissione europea.**

3. CONCLUSIONI: PROSPETTIVE

Con la tecnologia muta anche di continuo il modo in cui i dati personali vengono utilizzati e condivisi nella nostra società. Ciò pone al legislatore la sfida di definire un quadro giuridico che resista alla prova del tempo. Al termine del processo di riforma, le norme europee di protezione dei dati dovranno continuare ad assicurare un elevato livello di protezione e certezza giuridica a intere generazioni, pubbliche amministrazioni e imprese nel mercato interno. Per quanto complessa possa essere una situazione o sofisticata una tecnologia, occorre fare chiarezza sulle norme e sugli standard applicabili, la cui attuazione spetta alle autorità nazionali e al cui rispetto sono tenuti sia le imprese che gli ideatori di nuove tecnologie. Analogamente, dovranno essere chiari anche i diritti di cui godono gli interessati.

L'**approccio globale messo a punto dalla Commissione** per affrontare i problemi e conseguire gli obiettivi chiave individuati nella presente comunicazione servirà da base per il futuro dibattito con le altre istituzioni europee e le altre parti interessate, per essere successivamente tradotto in proposte e misure concrete di natura legislativa e non legislativa. A tal fine la Commissione auspica un riscontro sulle problematiche esposte nella presente comunicazione.

Su tale base, a seguito di una valutazione d'impatto e vista la Carta dei diritti fondamentali dell'Unione europea, la Commissione **proporrà un atto legislativo nel 2011** per la revisione del quadro giuridico sulla protezione dei dati, con l'intento di consolidare la posizione dell'UE nei confronti della protezione dei dati personali in tutte le politiche europee, anche nelle attività di contrasto e nella prevenzione della criminalità, considerate le specificità di questi due settori. In parallelo saranno messe a punto misure non legislative come la promozione dell'autoregolazione e lo studio della fattibilità di marchi europei di certificazione.

[51] Cfr. la nota 47.

In un secondo tempo la Commissione **valuterà se occorra adeguare altri atti legislativi** al nuovo quadro giuridico generale. Sarà interessato anzitutto il regolamento (CE) n. 45/2001, di cui bisognerà adattare le disposizioni. In una fase ulteriore occorrerà altresì esaminare attentamente le implicazioni per altri strumenti settoriali.

La Commissione continuerà poi ad assicurare un adeguato controllo della corretta applicazione del diritto dell'Unione in questo ambito, attuando una **politica attiva contro le infrazioni** ogni qualvolta non siano correttamente attuate e applicate le norme europee di protezione dei dati. In effetti la revisione attuale degli strumenti giuridici pertinenti non incide minimamente sull'obbligo degli Stati membri di attuare e assicurare la corretta applicazione degli strumenti legislativi esistenti in materia di protezione dei dati personali[52].

Niente più di un livello elevato e uniforme di protezione dei dati all'interno dell'Unione potrà difendere e promuovere meglio le norme europee di protezione dei dati a livello globale.

[52] Tra questi figura anche la decisione quadro 2008/977/GAI del Consiglio, alla quale gli Stati membri sono tenuti a conformarsi entro il 27 novembre 2010.