COMMISSIONE EUROPEA

Bruxelles, 25.1.2012
COM(2012) 9 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Salvaguardare la privacy in un mondo interconnesso
Un quadro europeo della protezione dei dati per il XXI secolo

(Testo rilevante ai fini del SEE)

[…]

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Salvaguardare la privacy in un mondo interconnesso
Un quadro europeo della protezione dei dati per il XXI secolo

(Testo rilevante ai fini del SEE)

1. LA PROTEZIONE DEI DATI PERSONALI NEL MONDO D'OGGI

La rapida evoluzione tecnologica e la globalizzazione hanno profondamente trasformato le modalità con cui sono raccolte, consultate, utilizzate e trasferite quantità sempre maggiori di dati personali. Nuove forme di condivisione delle informazioni attraverso i social network e di conservazione a distanza di grandi volumi di dati sono entrate nelle abitudini di molti dei 250 milioni di utenti Internet in Europa. Nel contempo, i dati personali sono diventati una risorsa per molte imprese le cui attività economiche spesso consistono in larga misura nella raccolta, aggregazione e analisi dei dati dei potenziali clienti[1].

Nel nuovo mondo digitale è **diritto di chiunque avere il controllo effettivo delle proprie informazioni personali**. La protezione dei dati è un diritto fondamentale in Europa, sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea e dall'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE) e, in quanto tale, deve essere tutelato.

La mancanza di fiducia frena i consumatori dall'acquistare online e dall'utilizzare nuovi servizi. Garantire un livello elevato di protezione dei dati è pertanto essenziale per aumentare la fiducia dei consumatori nei servizi online e realizzare il potenziale dell'economia digitale, promuovendo così **la crescita economica e la competitività delle industrie europee**.

Perché i dati possano circolare liberamente da uno Stato membro all'altro, l'Unione europea ha bisogno di norme moderne e coerenti, valide sul suo intero territorio, e le imprese hanno bisogno di regole chiare e uniformi che garantiscano la certezza del diritto e riducano al minimo gli oneri amministrativi. È questa la premessa essenziale perché il mercato interno funzioni correttamente e possa conseguentemente stimolare la crescita economica, creare occupazione e promuovere l'innovazione[2]. Modernizzare le norme dell'UE in materia di protezione dei dati, per rafforzarne la dimensione di mercato interno, garantire alle persone fisiche un'elevata protezione

---

1 Il mercato dell'analisi di grandi volumi di dati registra una crescita del 40% annuo in tutto il mondo: http://www.mckinsey.com/mgi/publications/big_data/.

2 Cfr. anche le conclusioni del Consiglio europeo del 23 ottobre 2011, che ha sottolineato il "ruolo chiave" del mercato unico nel creare crescita e occupazione e la necessità di completare il mercato unico digitale entro il 2015.

dei dati personali e promuovere la certezza del diritto, la chiarezza e la coerenza nell'applicazione, rientra pertanto tra le componenti chiave del piano d'azione della Commissione per l'attuazione del programma di Stoccolma[3] e dell'Agenda digitale europea[4] e, più in generale, della strategia Europa 2020[5] dell'UE.

La direttiva dell'UE del 1995[6], il principale strumento legislativo per la protezione dei dati personali in Europa, è stata una pietra miliare nella storia della protezione dei dati, i cui obiettivi - assicurare il funzionamento del mercato unico e l'effettiva protezione dei diritti e delle libertà fondamentali delle persone fisiche - rimangono tuttora validi. La direttiva risale tuttavia a 17 anni fa, un'epoca in cui Internet era ancora in uno stadio iniziale di sviluppo. Nel nuovo, dinamico, ambiente digitale le norme attualmente in vigore non permettono il grado di armonizzazione richiesto né hanno l'efficacia necessaria per garantire il diritto alla protezione dei dati di carattere personale. Per questo motivo la Commissione europea intende proporre una riforma radicale del quadro dell'UE in materia di protezione dei dati.

Inoltre, il trattato di Lisbona ha introdotto, con l'articolo 16 del TFUE, una nuova base giuridica per un approccio moderno e globale alla protezione dei dati e alla libera circolazione dei dati di carattere personale, che copre anche la cooperazione di polizia e giudiziaria in materia penale[7]. Tale approccio si evince anche dalle comunicazioni della Commissione europea relative al programma di Stoccolma e al piano d'azione di Stoccolma[8], che sottolineano l'importanza per l'Unione di "introdurre un regime completo in materia di protezione dei dati personali che ricomprenda tutte le competenze dell'Unione" e di "assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati."

Per assicurare un processo trasparente di riforma del quadro dell'UE in materia di protezione dei dati, la Commissione ha avviato consultazioni pubbliche fin dal 2009[9] e condotto un dialogo approfondito con le parti interessate[10]. Il 4 novembre 2010 la Commissione ha pubblicato la comunicazione "Un approccio globale alla protezione dei dati personali nell'Unione europea"[11] che esponeva i temi principali della riforma. Tra settembre e dicembre 2011 la Commissione ha inoltre preso parte ad un dialogo serrato con le autorità nazionali di protezione dei dati in Europa, da un lato, e con il garante europeo della protezione dei dati, dall'altro, finalizzato ad esaminare le

---

3 COM(2010) 171 definitivo.

4 COM(2010) 245 definitivo.

5 COM(2010) 2020 definitivo.

6 Direttiva 95/46/CE 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).

7 Con decisione del Consiglio basata sull'articolo 39 del TUE saranno stabilite norme specifiche per il trattamento di dati a cura degli Stati membri nel settore della politica estera e di sicurezza comune.

8 COM(2009) 262 e COM(2010) 171.

9 Le consultazioni pubbliche sono state due: la prima da luglio a dicembre 2009 (http://ec.europa.eu/culture/news/consulting_public/news_consulting_0003_en.htm) e la seconda da novembre 2010 a gennaio 2011 (http://ec.europa.eu/culture/news/consulting_public/news_consulting_6_en.htm).

10 Nel 2010 sono stati organizzati specifici incontri con le autorità degli Stati membri e le parti interessate del settore privato. Nel novembre 2010 Viviane Reding, commissaria per la giustizia, ha organizzato una tavola rotonda sulla riforma della protezione dei dati. Nel corso del 2011 si sono svolti altri workshop e seminari su questioni specifiche (quali la notificazione delle violazioni dei dati).

11 COM(2010)609.

opzioni che garantissero un'applicazione più coerente delle norme dell'UE in tutti gli Stati membri[12].

Tali discussioni hanno messo chiaramente in evidenza che tanto i cittadini quanto le imprese desiderano che la Commissione europea proceda a una riforma completa delle norme dell'UE sulla protezione dei dati. Dopo aver valutato le conseguenze delle diverse opzioni strategiche[13], la Commissione europea propone ora un **quadro normativo solido e coerente, trasversale a tutte le politiche dell'Unione, che rafforza i diritti delle persone fisiche, consolida la dimensione di mercato interno della protezione dei dati e riduce gli oneri amministrativi che gravano sulle imprese**[14]. La Commissione propone un nuovo quadro composto da:

– un **regolamento** che sostituisce la direttiva 95/46/CE e istituisce un quadro europeo generale in materia di protezione dei dati[15];

– e una **direttiva** che sostituisce la decisione quadro 2008/977/GAI[16] e stabilisce le norme applicabili alla protezione dei dati personali trattati ai fini di **prevenzione, indagine, accertamento o perseguimento dei reati e relative attività giudiziarie**.

La presente comunicazione illustra gli elementi principali della riforma del quadro dell'UE per la protezione dei dati.

2. DARE ALLE PERSONE IL CONTROLLO DEI PROPRI DATI PERSONALI

La direttiva 95/46/CE, il principale atto legislativo in vigore nell'UE in materia di protezione dei dati, non armonizza sufficientemente in tutti gli Stati membri le modalità di esercizio del diritto alla protezione dei dati da parte delle persone fisiche, né le competenze conferite alle autorità nazionali di protezione dei dati sono sufficientemente armonizzate per garantire l'applicazione coerente ed efficace delle norme. Ciò significa che nella pratica far valere tali diritti, soprattutto online, è più difficile in alcuni Stati membri rispetto ad altri.

---

12 Cfr. la lettera della commissaria UE per la giustizia, Viviane Reding, del 19 settembre 2011 ai membri del gruppo di lavoro "articolo 29", pubblicata all'indirizzo http://ec.europa.eu/culture//article-29 protezione dei dati/documentation/other-document/index_en.htm.

13 Cfr. la valutazione d'impatto SEC(2012) 72.

14 Ciò comporterà, in una fase successiva, le modifiche necessarie per conformare specifici strumenti settoriali come il regolamento (CE) n. 45/2001 (GU L 8 del 12.1.2001, pag. 1).

15 Inoltre, il regolamento prevede alcuni adattamenti tecnici della direttiva relativa alla vita privata e alle comunicazioni elettroniche (2002/58/CE) come da ultimo modificata dalla direttiva 2009/136/CE (GU L 337 del 18.12.2009, pag. 11), per tener conto della trasformazione in regolamento della direttiva 95/46/CE. Le conseguenze in materia di diritto sostanziale per la direttiva relativa alla vita privata e alle comunicazioni elettroniche prodotte dal nuovo regolamento e dalla nuova direttiva saranno oggetto, a tempo debito, di una revisione della Commissione, che terrà conto dei risultati emersi dai negoziati sulle proposte attuali con il Parlamento europeo e il Consiglio.

16 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). Una relazione sull'attuazione della decisione quadro da parte degli Stati membri (COM (2012) 12) è adottata contestualmente agli altri elementi del pacchetto di riforma legislativa in materia di protezione dei dati.

Tali difficoltà sono accentuate anche dall'enorme quantità di dati raccolti quotidianamente e dal fatto che spesso gli utenti non sono del tutto consapevoli di tale raccolta. Benché molti cittadini europei ritengano che la divulgazione dei dati personali faccia sempre più parte della vita moderna[17], il 72% degli internauti europei si inquieta per i troppi dati personali richiesti online[18]. A ciò si aggiunga che gli utenti hanno l'impressione di non aver alcun controllo dei propri dati, non sono adeguatamente informati della sorte riservata alle informazioni personali, dell'identità dei destinatari e della finalità della trasmissione e spesso ignorano le modalità per esercitare i loro diritti online.

"Diritto all'oblio"

Uno studente europeo membro di un social network decide di chiedere l'accesso a tutti i dati personali che lo riguardano e che la rete ha conservato. Si accorge in quella occasione che i dati raccolti dalla rete sono molti di più di quanto pensasse e che sono tuttora conservati dati personali che riteneva fossero stati rimossi.

La riforma delle norme dell'UE di protezione dei dati garantirà che ciò non si verifichi più, grazie all'introduzione dei seguenti obblighi:

- i servizi di socializzazione in rete (e tutti gli altri responsabili del trattamento) sono espressamente tenuti a ridurre al minimo il volume dei dati personali degli utenti che raccolgono e sottopongono a trattamento;

- i sistemi devono essere configurati con impostazioni prestabilite che garantiscano che i dati non siano resi pubblici;

- i responsabili del trattamento sono espressamente tenuti a cancellare i dati di chi ne faccia esplicita richiesta, in assenza di altri motivi legittimi che ne giustifichino la conservazione.

Nella fattispecie sopra illustrata, la normativa proposta obbligherebbe il provider di social network a rimuovere immediatamente e completamente i dati dello studente.

Come sottolineato nell'Agenda digitale europea, le preoccupazioni attinenti alla tutela della vita privata sono tra i motivi che più frequentemente frenano le persone dall'acquistare beni e servizi online. Considerando il contributo che il settore delle tecnologie dell'informazione e della comunicazione (TIC) apporta alla crescita globale della produttività in Europa – il 20% deriva direttamente dalle TIC e il 30% dagli investimenti nelle TIC[19] – la fiducia in tali servizi è fondamentale per stimolare la crescita dell'economia dell'Unione e la competitività dell'industria europea.

Notificazioni delle violazioni di dati

Dei pirati informatici hanno preso di mira un portale che offre servizi di giochi online ad utenti nell'Unione. L'attacco era rivolto alle banche dati contenenti informazioni personali (compresi nomi, indirizzi ed, eventualmente, estremi delle carte di credito) di decine di milioni di utenti in tutto il mondo. La società ha atteso una settimana prima di notificare la violazione dei dati agli utenti interessati.

---

17 Cfr. Speciale Eurobarometro 359 – Attitudes on Data Protection and Electronic Identity in the European Union, giugno 2011, pag. 23.

18 Idem, pag. 54.

19 Cfr. Agenda digitale europea, op. cit., pag. 4.

La riforma della normativa dell'Unione sulla protezione dei dati garantirà che ciò non si verifichi più. Le nuove norme obbligheranno le imprese:

- a rafforzare le loro misure di sicurezza volte a prevenire e impedire violazioni di dati;

- a notificare senza ingiustificato ritardo le violazioni di dati sia all'autorità nazionale di protezione dei dati (se possibile, entro 24 ore dalla scoperta della violazione) sia agli interessati.

Le nuove proposte legislative presentate dalla Commissione mirano a rafforzare i diritti delle persone fisiche, dotandole di strumenti efficaci e operativi atti a garantire che siano pienamente informate su quanto accade ai dati che le riguardano e a permettere un più efficace esercizio dei loro diritti.

Per rafforzare il diritto delle persone fisiche alla protezione dei dati, la Commissione propone nuove norme intese a:

consentire loro di controllare meglio i dati che le riguardano:

- prevedendo che, quando è richiesto, il **consenso** sia **espresso in modo esplicito, cioè manifestato mediante una dichiarazione o un'azione che richiede l'intervento attivo dell'interessato**, e sia manifestato liberamente;

- dotando gli utenti di Internet di un effettivo **diritto all'oblio** nell'ambiente online: ossia il diritto di far cancellare i dati che li riguardano quando revocano il consenso, in assenza di altri motivi legittimi che ne giustifichino la conservazione;

- garantendo loro un **facile accesso ai propri dati** e un **diritto alla portabilità degli stessi**: ossia il diritto di ottenere dal responsabile del trattamento una copia dei dati conservati e di trasferirli da un prestatore di servizi a un altro, senza impedimenti;

- rafforzando il **diritto di informazione**, affinché gli utenti siano pienamente consapevoli delle modalità di trattamento dei dati che li riguardano, specie se si tratta di **minori**.

migliorare i mezzi a disposizione delle persone fisiche per l'esercizio dei propri diritti:

- rafforzando **l'indipendenza e i poteri delle autorità nazionali di protezione dei dati**, di modo che siano adeguatamente attrezzate per dare efficace seguito ai reclami, compresi poteri di svolgere efficacemente indagini, adottare decisioni vincolanti e imporre sanzioni efficaci e dissuasive;

- migliorando i **mezzi di ricorso in sede amministrativa e giudiziaria** in caso di **violazione** dei diritti relativi alla protezione dei dati; in particolare, le associazioni autorizzate potranno agire in giudizio per conto dell'interessato.

rafforzare la sicurezza dei dati:

- incoraggiando l'utilizzo di **tecnologie che rafforzano la privacy** (*tecnologie che proteggono la riservatezza delle informazioni riducendo al minimo la memorizzazione dei dati personali*), e di **impostazioni di default orientate alla privacy** e **sistemi di certificazione della privacy**;

- introducendo un **obbligo generale**[20] che impone ai responsabili del trattamento di **notificare senza indugio** le violazioni di dati alle autorità di protezione dei dati (se possibile entro 24 ore) e agli interessati.

aumentare la rendicontazione di coloro che trattano dati, in particolare:

- i responsabili del trattamento saranno tenuti a designare un **responsabile della protezione dei dati** nelle imprese con oltre 250 dipendenti e nelle imprese che partecipano a trattamenti che, per loro natura, oggetto o finalità, presentano rischi specifici per i diritti e le libertà delle persone (trattamenti rischiosi);

- introducendo il **principio di "protezione dei dati sin dalla progettazione**" per far sì che le garanzie in materia di protezione dei dati siano incorporate già in fase di progettazione nelle procedure e nei sistemi di trattamento;

- le organizzazioni che effettuano trattamenti a rischio saranno tenute a realizzare **valutazioni d'impatto sulla protezione dei dati**.

3. NORME IN MATERIA DI PROTEZIONE DEI DATI ADATTE AL MERCATO INTERNO DIGITALE

Benché l'attuale direttiva si prefigga di garantire un livello equivalente di protezione dei dati in tutta l'Unione, tra i vari Stati membri persistono notevoli differenze quanto a norme applicate. Di conseguenza, i responsabili del trattamento possono trovarsi di fronte a 27 legislazioni e requisiti nazionali diversi all'interno dell'Unione. Ne risulta un **quadro normativo frammentato**, che genera **incertezza giuridica** e porta a una protezione diseguale delle persone fisiche. Tale situazione produce **costi inutili e oneri amministrativi** per le imprese e disincentiva le imprese che operano nel mercato interno dall'espandere le loro attività all'estero.

Le risorse e i poteri delle autorità nazionali di protezione dei dati variano sensibilmente da uno Stato membro all'altro[21]. In alcuni casi ciò significa che tali autorità non sono in grado di esercitare i compiti di controllo in modo soddisfacente. La cooperazione tra le autorità nazionali di protezione dei dati a livello europeo – attraverso l'attuale gruppo consultivo (gruppo di lavoro "articolo 29")[22] – non garantisce sempre un'applicazione coerente della normativa e pertanto occorre migliorarla.

Applicazione coerente delle norme sulla protezione dei dati in Europa

Una multinazionale con più stabilimenti nell'Unione ha messo in atto un sistema di mappatura elettronica in Europa che raccoglie immagini di tutti gli edifici pubblici e privati, e può anche

20 Attualmente obbligatorio soltanto nel settore delle telecomunicazioni, in forza della direttiva e-Privacy.

21 Per ulteriori dettagli su tale aspetto, si veda la valutazione d'impatto che correda la proposta giuridica, SEC (2012) 72.

22 Il Gruppo di lavoro "articolo 29" è stato istituito nel 1996 (dall'articolo 29 della direttiva 95/46/CE); 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. Per maggiori informazioni sulle sue attività, si consulti il sito: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

fotografare le persone di passaggio sulla pubblica via. In uno Stato membro l'inclusione di immagini non sfuocate di persone ignare di essere state fotografate è considerata illecita, mentre in altri Stati membri ciò non costituisce un'infrazione alla legislazione in materia di protezione dei dati. Di conseguenza le autorità nazionali di protezione dei dati non hanno potuto adottare una posizione coerente per risolvere il problema.

A seguito della riforma della normativa dell'Unione sulla protezione dei dati tale situazione non potrà più verificarsi in futuro, in quanto:

- i criteri e le garanzie di protezione dei dati saranno stabiliti da un regolamento dell'Unione direttamente applicabile in tutto il territorio UE;

- solo l'autorità di protezione dei dati nello Stato membro in cui la società ha lo stabilimento principale sarà competente a pronunciarsi sulla legittimità del comportamento;

- un coordinamento rapido ed efficace tra autorità nazionali di protezione dei dati - poiché il servizio è rivolto a persone fisiche in diversi Stati membri – contribuirà a garantire che le nuove norme dell'UE sulla protezione dei dati siano applicate e fatte rispettare in modo uniforme in tutti gli Stati membri.

Per garantire la coerente applicazione e, in ultima analisi, l'applicazione uniforme delle norme in tutta l'Unione occorre rafforzare le autorità nazionali e intensificarne la cooperazione.

Un quadro normativo solido, chiaro e uniforme a livello dell'Unione contribuirà a realizzare il potenziale del mercato interno digitale e a promuovere la crescita economica, l'innovazione e la creazione di posti di lavoro. L'adozione di un regolamento ovvierà alla frammentazione dei regimi giuridici di 27 Stati membri ed eliminerà gli ostacoli all'ingresso nel mercato, condizione di particolare importanza per le micro, piccole e medie imprese.

Grazie alle nuove regole le imprese europee godranno inoltre di un vantaggio nella concorrenza a livello mondiale. Nel nuovo quadro normativo potranno infatti offrire ai propri clienti la garanzia che tratteranno con la debita cura e diligenza le loro importanti informazioni personali. La fiducia in un regime normativo coerente, a livello di UE, costituirà un elemento fondamentale per i prestatori di servizi e un incentivo per gli investitori alla costante ricerca di condizioni ottimali per l'ubicazione dei loro servizi.

Per rafforzare la **dimensione di mercato interno della protezione dei dati**, la Commissione propone di:

- adottare norme che disciplinano la protezione dei dati a livello dell'UE attraverso un **regolamento direttamente applicabile in tutti gli Stati membri**[23], che metterà fine all'applicazione simultanea e cumulativa di diverse legislazioni nazionali in materia. Le imprese realizzeranno in tal modo un **risparmio netto di circa 2,3 miliardi di euro l'anno soltanto in termini di minori oneri amministrativi**;

[23] La Commissione presenta anche una proposta di direttiva intesa a definire le disposizioni applicabili al settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale (cfr. punto 4 infra), che darà agli Stati membri una maggiore flessibilità in questo settore specifico.

- **semplificare il contesto normativo riducendo sensibilmente la burocrazia** ed eliminando **formalità** quali gli obblighi generali di notificazione, (con un risparmio netto annuo di 130 milioni di euro solo in termini di minori oneri amministrativi). Data la loro importanza per la competitività dell'economia europea, un'attenzione particolare è rivolta alle esigenze specifiche delle micro, piccole e medie imprese;

- **accrescere l'indipendenza e i poteri delle autorità nazionali di protezione dei dati** per consentire loro di svolgere indagini, adottare decisioni vincolanti e imporre sanzioni efficaci e dissuasive, e obbligare gli Stati membri a dotarle delle **risorse sufficienti** per eseguire i loro compiti;

- **istituire un sistema di "sportello unico" per la protezione dei dati nell'UE:** i responsabili del trattamento nell'UE avranno come interlocutore **un'unica autorità di protezione dei dati**, ossia quella dello Stato membro in cui si trova lo stabilimento principale della società;

- creare le condizioni per una **cooperazione agile ed efficace tra autorità di protezione dei dati,** che comprendano l'obbligo per una autorità di svolgere indagini e ispezioni su richiesta di un'altra e l'obbligo di riconoscere le reciproche decisioni;

- **istituire un meccanismo che garantisca la coerenza** a livello dell'Unione, affinché le decisioni delle autorità di protezione dei dati con maggiore impatto europeo tengano pienamente conto dei pareri espressi dalle altre autorità di protezione dei dati interessate e siano pienamente conformi al diritto dell'Unione;

- promuovere lo status del gruppo di lavoro "articolo 29", trasformandolo in un **comitato europeo per la protezione dei dati indipendente**, al fine di rafforzare il suo contributo all'applicazione coerente della normativa in materia di protezione dei dati, fornire una solida base di cooperazione tra autorità di protezione dei dati, compreso il garante europeo della protezione dei dati, e potenziare le sinergie e l'efficienza, prevedendo che le funzioni di segreteria del comitato europeo della protezione dei dati siano assicurate dal garante europeo della protezione dei dati.

Il nuovo regolamento dell'Unione garantirà una protezione efficace del diritto fondamentale alla protezione dei dati in tutta l'Unione europea e rafforzerà il funzionamento del mercato interno. Allo stesso tempo – in considerazione del fatto che, come sottolineato dalla Corte di giustizia dell'Unione europea[24], il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale[25] e va contemperato con altri diritti fondamentali, in

---

24 Cause riunite C-92/09 e C-93/09: Sentenza della Corte di giustizia dell'Unione europea 9 novembre 2010 - Volker und Markus Schecke e Eifert, Racc. 2010, pag. I-0000, non disponibile ancora nella pubblicazione ufficiale.

25 Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio del diritto alla protezione dei dati devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

ottemperanza al principio di proporzionalità[26] – il regolamento contiene specifici riferimenti alle disposizioni che assicurano il rispetto di altri diritti fondamentali, quali il diritto alla libertà di espressione e d'informazione, i diritti della difesa, il diritto al segreto professionale (ad esempio per le professioni legali), senza pregiudicare lo status accordato alle chiese dalle legislazioni nazionali degli Stati membri.

4. L'USO DI DATI NELLA COOPERAZIONE DI POLIZIA E GIUDIZIARIA IN MATERIA PENALE

L'entrata in vigore del trattato di Lisbona e, in particolare, l'introduzione di una nuova base giuridica (articolo 16 TFUE), consente di istituire un quadro completo in materia di protezione dei dati per garantire un elevato livello di protezione dei dati delle persone fisiche, nel rispetto delle specificità del settore della cooperazione di polizia e giudiziaria in materia penale. In particolare, il nuovo quadro dell'UE sulla protezione dei dati può applicarsi ai trattamenti sia nazionali che transfrontalieri di dati personali. Ciò ridurrà le divergenze tra legislazioni nazionali, a beneficio della protezione dei dati personali nel suo insieme. Questa nuova situazione potrebbe anche contribuire ad agevolare lo scambio di informazioni tra le autorità nazionali di polizia e giudiziarie e migliorare la cooperazione nella lotta contro le forme gravi di criminalità in Europa. Il trattamento dei dati da parte di autorità di polizia e giudiziaria in materia penale è al momento principalmente disciplinato dalla decisione quadro 2008/977/GAI, anteriore all'entrata in vigore del trattato di Lisbona. Trattandosi di una decisione quadro, la Commissione non dispone in questo caso di un potere coercitivo, il che ha contribuito ad un'attuazione ineguale tra Stati membri. Il campo di applicazione della decisione quadro è inoltre limitato alle attività di trattamento transfrontaliere.[27] Ciò significa che il trattamento di dati personali che non sono oggetto di scambio non è attualmente contemplato dalla normativa dell'UE che disciplina i trattamenti di dati e tutela il diritto fondamentale alla protezione dei dati. Ne conseguono inoltre, in alcuni casi, difficoltà di ordine pratico per la polizia e le altre autorità, per le quali può non essere agevole stabilire il carattere puramente nazionale o transfrontaliero di un trattamento di dati né prevedere se i dati "nazionali" possano essere oggetto di un successivo scambio transfrontaliero.[28]

Il nuovo quadro normativo della protezione dei dati mira pertanto a garantire un livello uniforme ed elevato di protezione dei dati per **aumentare la fiducia reciproca tra le autorità di polizia e giudiziarie di diversi Stati membri, facilitando così la libera circolazione dei dati, nonché l'efficacia della cooperazione tra tali autorità**.

---

[26] Causa C-101/01: Sentenza della Corte di giustizia dell'Unione europea 6.11.2003 - Lindqvist, Racc. 2003, pag. I-12971, paragrafi 82-90; Causa C-73/07, sentenza del 16.12.2008; Satamedia, Racc. 2008, pag. I-9831, paragrafi 50-62.

[27] Più precisamente, la decisione quadro si applica ai dati personali che sono o sono stati trasmessi o resi disponibili tra Stati membri o oggetto di scambio tra gli Stati membri e le istituzioni e gli organi dell'UE (cfr. articolo 1, paragrafo 2).

[28] Ciò è stato confermato da alcuni Stati membri nelle risposte al questionario della Commissione concernente la relazione sull'attuazione della decisione quadro (COM (2012) 12).

Per garantire un elevato livello di protezione dei dati personali nell'ambito della cooperazione di polizia e giudiziaria in materia penale e agevolare lo scambio di tali dati tra le autorità nazionali a ciò preposte, la Commissione propone, nell'ambito del pacchetto di riforma in materia di protezione dei dati, una direttiva che:

- **applicherà i principi generali di protezione dei dati** alla cooperazione di polizia e alla cooperazione giudiziaria in materia penale, nel rispetto delle specificità di tali settori[29];

- stabilirà **condizioni e criteri minimi armonizzati da applicare ad eventuali limitazioni** alle norme generali. Ciò riguarda, in particolare, i diritti delle persone fisiche di essere informate se le autorità di polizia o giudiziarie consultano o elaborano dati che le riguardano. Tali limitazioni sono necessarie per efficaci operazioni di prevenzione, indagine, accertamento e perseguimento di reati;

- istituirà un regime speciale per tenere conto della specifica natura delle attività di contrasto, ivi compresa la distinzione tra diverse categorie di interessati i cui diritti possono variare (ad esempio i testimoni e gli indiziati).

5. PROTEZIONE DEI DATI NEL CONTESTO DELLA GLOBALIZZAZIONE

I diritti delle persone devono continuare ad essere garantiti anche quando i dati personali sono trasferiti dall'Unione europea verso paesi terzi, e ogniqualvolta dati personali relativi a persone residenti negli Stati membri sono utilizzati o analizzati da fornitori di servizi di paesi terzi. Ciò significa che le norme dell'UE in materia di protezione dei dati si applicano indipendentemente dall'ubicazione geografica di una società o dallo stabilimento in cui avviene il trattamento dei dati.

Nel contesto dell'odierna globalizzazione i dati personali sono trasferiti attraverso un numero crescente di frontiere virtuali e geografiche e conservati su server ubicati in più paesi. Sempre più società informatiche offrono servizi di "cloud computing", che consentono ai clienti di accedere e conservare i dati su server remoti. Tali sviluppi impongono di migliorare gli attuali meccanismi di trasferimento di dati verso paesi terzi, con decisioni di adeguatezza – ossia decisioni che certificano che le norme sulla protezione dei dati di un paese terzo sono "adeguate" – e garanzie appropriate, quali clausole contrattuali tipo o norme vincolanti d'impresa[30], per assicurare un'elevata protezione dei dati nei trattamenti internazionali e facilitare la circolazione dei dati oltre frontiera.

---

29 Cfr. Dichiarazione n. 21, relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, come allegato all' atto finale della conferenza intergovernativa che ha adottato il trattato di Lisbona.

30 Le norme vincolanti d'impresa sono codici di pratiche basate sulle norme europee per la protezione dei dati, approvati da almeno un'autorità di protezione dei dati, che le organizzazioni elaborano su base volontaria e applicano per assicurare adeguate garanzie di sicurezza per le categorie di trasferimenti di dati personali tra imprese che sono parte dello stesso gruppo di società, e che sono vincolate da tali norme. Tali norme non sono esplicitamente contemplate dalla direttiva 95/46/CE, ma si sono sviluppate nella pratica tra autorità di protezione di dati con il sostegno del gruppo di lavoro "articolo 29".

Norme vincolanti d'impresa

Un gruppo di società deve trasferire periodicamente dati personali dalle sue affiliate con sede nell'Unione a quelle situate in paesi terzi. Il gruppo propone di introdurre un corpus di norme vincolanti d'impresa per conformarsi alla legislazione dell'Unione limitando al contempo gli obblighi amministrativi per ogni singolo trasferimento. Nella pratica, le norme vincolanti d'impresa garantiscono l'applicazione di un unico corpus di regole in tutto il gruppo, senza dover concludere diversi contratti a livello interno.

Conformemente alle pratiche correnti stabilite in seno al gruppo di lavoro "articolo 29", il riconoscimento dell'adeguatezza delle garanzie previste dalle norme vincolanti d'impresa di una società presuppone un controllo approfondito da parte di tre autorità di protezione dei dati (un'autorità "capofila" e due autorità "esaminatrici") ma anche altre autorità possono esprimere le proprie osservazioni. Le legislazioni di molti Stati membri richiedono inoltre ulteriori autorizzazioni nazionali per i trasferimenti soggetti alle norme vincolanti d'impresa, il che rende il processo di adozione di tali norme molto laborioso, costoso, lungo e complesso.

A seguito della riforma della protezione dei dati:

- questo processo sarà più semplice e razionalizzato;

- le norme vincolanti d'impresa saranno convalidate da un'unica autorità di protezione dei dati, con meccanismi atti a garantire un rapido coinvolgimento di altre autorità di protezione dei dati;

- una volta approvate da un'autorità di protezione dei dati, le norme vincolanti d'impresa saranno valide in tutto il territorio dell'UE senza ulteriori autorizzazioni a livello nazionale.

Per **affrontare le sfide della globalizzazione**, occorrono meccanismi e strumenti flessibili, in particolare per le imprese operanti a livello mondiale – pur garantendo nel contempo una protezione completa e senza lacune dei dati personali. La Commissione propone le seguenti misure:

- **norme chiare** che stabiliscano in quali casi **il diritto dell'Unione si applica ai responsabili del trattamento stabiliti in paesi terzi**, precisando in particolare che, ogni volta che i prodotti e i servizi sono offerti a persone fisiche nell'Unione o che viene analizzato il comportamento di dette persone, **si applicano le norme europee**;

- la Commissione europea adotterà ogni **decisione relativa all'adeguatezza del livello di protezione dei dati** sulla base di criteri chiari ed espliciti, anche nel settore della **cooperazione di polizia e giudiziaria in materia penale**;

- i flussi legali di dati verso i paesi terzi saranno agevolati grazie al rafforzamento e alla semplificazione delle **norme relative ai trasferimenti internazionali** di dati verso paesi non oggetto di decisioni di adeguatezza; ciò avverrà in particolare razionalizzando e estendendo il ricorso a strumenti quali le **norme vincolanti d'impresa**, in modo che possano essere applicati ai **responsabili del trattamento**, nonché all'interno dei **gruppi di imprese**, tenendo così conto del numero crescente di società che effettuano attività di trattamento dei dati, in particolare nel settore del *cloud computing*;

- intraprendere un **dialogo** e, se del caso, **negoziati** con i paesi terzi, in particolare con i partner strategici dell'Unione e i paesi interessati dalla politica europea di vicinato, e le organizzazioni internazionali interessate (per esempio, il Consiglio d'Europa, l'Organizzazione per la cooperazione e lo sviluppo economico,

le Nazioni Unite) al fine di **promuovere elevati standard di protezione dei dati, interoperabili** a livello mondiale.

6. CONCLUSIONE

La riforma della protezione dei dati mira a realizzare un **quadro globale, coerente, solido e moderno per la protezione dei dati nell'Unione europea**. Il diritto fondamentale delle persone alla protezione dei dati ne sarà rafforzato. Altri diritti, quali la libertà di espressione e d'informazione, i diritti del minore, la libertà d'impresa, il diritto a un giudice imparziale e al segreto professionale (ad esempio per le professioni legali) e lo status delle chiese definito dalle legislazioni degli Stati membri saranno rispettati.

La riforma andrà innanzitutto a beneficio delle persone fisiche, rafforzando i loro diritti alla protezione dei dati e la loro fiducia nell'ambiente digitale; semplificherà inoltre notevolmente il quadro giuridico per le imprese e il settore pubblico. Ciò dovrebbe stimolare lo sviluppo dell'economia digitale in tutto il mercato interno dell'UE e oltre, in linea con gli obiettivi della strategia Europa 2020 e dell'Agenda digitale europea. Infine, la riforma aumenterà la fiducia tra le autorità di contrasto e faciliterà gli scambi di informazioni e la cooperazione tra le autorità stesse nella lotta contro le forme gravi di criminalità, garantendo nel contempo alle persone fisiche un livello elevato di protezione.

La Commissione europea lavorerà a stretto contatto con il Parlamento europeo e il Consiglio per la conclusione, entro fine 2012, di un accordo sul nuovo quadro della protezione dei dati. Nel corso del processo di adozione e oltre, in particolare nel contesto dell'attuazione dei nuovi strumenti giuridici, la Commissione proseguirà il **dialogo diretto** e **trasparente con tutte le parti interessate**, tra cui rappresentanti del settore pubblico e privato, compresi rappresentanti del sistema giudiziario e delle forze di polizia, delle autorità di regolamentazione delle comunicazioni elettroniche, delle organizzazioni della società civile, delle autorità di protezione dei dati ed esponenti del mondo accademico, nonché di agenzie specializzate dell'UE, quali Eurojust, Europol, l'Agenzia per i diritti fondamentali, e l'Agenzia europea per la sicurezza delle reti e dell'informazione.

In un contesto di evoluzione costante delle tecnologie dell'informazione e dei comportamenti sociali, il dialogo è fondamentale per ricevere i contributi necessari a garantire un elevato livello di protezione delle persone, la crescita e la competitività delle imprese nell'Unione, l'efficacia operativa del settore pubblico (compresi gli organismi di polizia e il sistema giudiziario) e il minor livello possibile di burocrazia.