servizio affari internazionali
ufficio dei rapporti con le istituzioni dell'Unione europea

SCHEDA DI VALUTAZIONE n. 22/2012
dei progetti di atti legislativi trasmessi ai sensi del protocollo sull'applicazione dei principi di sussidiarietà e proporzionalità

TITOLI:	Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati). Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati.		
NUMERO ATTI	COM (2012) 11 def. COM (2012) 10 def.		
NUMERO PROCEDURE	2012/0011 (COD) 2012/0010 (COD)		
AUTORE	Commissione europea		
DATA DEGLI ATTI	25/01/2012		
DATE DI TRASMISSIONE	14/02/2012; 13/02/2012		
SCADENZE OTTO SETTIMANE	10/04/2012		
ASSEGNATI IL	16/02/2012		
COMM.NE DI MERITO	2ª	**Parere motivato entro**	22/03/2012
COMM.NI CONSULTATE	1ª, 3ª e 14ª	**Oss.ni e proposte entro**	15/03/2012
OGGETTO	La proposta di regolamento e la proposta di direttiva in esame (COM (2012) 11 e COM (2012) 10) mirano a instaurare un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione che, affiancato da efficaci misure di attuazione, consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà alle persone fisiche il controllo dei loro dati personali e rafforzerà la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche, obiettivi che rientrano tra le componenti chiave del piano d'azione della		

Commissione per l'attuazione del programma di Stoccolma[1] e dell'Agenda digitale europea[2] e, più in generale, della strategia Europa 2020[3] dell'UE.

Il quadro giuridico attuale si basa sulla direttiva 95/46/CE[4], adottata nel 1995 per salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri, e sulla decisione quadro 2008/977/GAI, uno strumento generale applicabile a livello di Unione per proteggere i dati personali nei settori della cooperazione di polizia e giudiziaria in materia penale[5].

BASE GIURIDICA

La base giuridica della proposta di regolamento è individuata nell'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE) che stabilisce il principio secondo il quale ogni persona ha diritto alla protezione dei dati di carattere personale. Il regolamento è considerato lo strumento più idoneo per definire il quadro giuridico per la protezione dei dati personali nell'UE. L'applicabilità diretta di un regolamento ai sensi dell'articolo 288 del TFUE ridurrà la frammentazione giuridica e offrirà maggiore certezza giuridica grazie all'introduzione di una serie di norme di base armonizzate, migliorando la tutela dei diritti fondamentali delle persone fisiche e contribuendo al corretto funzionamento del mercato interno.

Quanto alla proposta di direttiva, l'articolo 16, paragrafo 2 del TFUE introduce una base giuridica specifica per l'adozione di norme in materia di protezione dei dati personali, anche nell'ambito della cooperazione di polizia e giudiziaria in materia penale. La proposta di direttiva è finalizzata a tutelare i diritti e le libertà fondamentali delle persone fisiche e in particolare il diritto alla protezione dei dati personali, garantendo al tempo stesso lo scambio di dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e contribuendo a una più efficace cooperazione nella lotta contro la criminalità in Europa.

Inoltre va ricordato che l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea annovera la protezione dei dati personali tra i diritti fondamentali.

PRINCIPI DI SUSSIDIARIETÀ E PROPORZIONALITÀ

La Commissione ritiene le due proposte conformi al **principio di sussidiarietà**, in quanto il diritto alla protezione dei dati personali, sancito dall'articolo 8 della Carta dei diritti fondamentali, richiede il medesimo livello di protezione dei dati stessi in tutta l'Unione. In mancanza di una normativa

[1] COM(2010) 171 definitivo.
[2] COM(2010) 245 definitivo.
[3] COM(2010) 2020 definitivo.
[4] 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).
[5] 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).

dell'Unione si rischierebbe di instaurare livelli diversi di protezione negli Stati membri e di creare restrizioni nei flussi transfrontalieri di dati personali tra gli Stati membri dotati di norme differenti, considerando che i dati personali sono trasferiti attraverso le frontiere nazionali, sia interne che esterne, ad un ritmo sempre crescente anche ai fini della prevenzione e della lotta contro la criminalità e il terrorismo transnazionale. Inoltre, esistono difficoltà pratiche nell'attuare efficacemente la normativa in materia di protezione dei dati e occorre stabilire una cooperazione tra gli Stati membri e le autorità nazionali a livello di Unione, per garantire uniformità nell'applicazione del diritto dell'UE. Infine, l'Unione si trova nella posizione migliore per garantire in maniera efficace e coerente lo stesso livello di protezione alle persone fisiche i cui dati personali siano trasferiti verso paesi terzi. Gli Stati membri non sono in grado da soli di risolvere i problemi posti dalla situazione attuale, in particolare dalla frammentazione delle legislazioni nazionali. Conseguentemente esiste la precisa esigenza di istituire un quadro armonizzato e coerente che consenta un agevole trasferimento transfrontaliero di dati personali all'interno dell'Unione europea e che garantisca nel contempo un'effettiva tutela di tutte le persone fisiche nell'intero territorio dell'UE.

Le due proposte sono altresì conformi al **principio di proporzionalità** in quanto gli interventi previsti sono mirati e si limitano a quanto strettamente necessario per conseguire gli obiettivi richiesti.

ANNOTAZIONI:

Le due proposte in esame prendono le mosse dalla necessità di un nuovo quadro giuridico per la protezione dei dati personali nell'Unione europea, come delineato nella comunicazione COM (2012) 9 (*Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo)* e sono il risultato di estese consultazioni con tutte le principali parti interessate sul riesame dell'attuale quadro normativo in materia di protezione dei dati personali, svoltesi nell'arco di oltre due anni e comprendenti una conferenza ad alto livello nel maggio 2009 e due fasi di consultazione pubblica[6].

Nel corso delle consultazioni sull'impostazione generale la grande maggioranza degli interpellati ha convenuto sulla necessità di garantire un'applicazione più coerente della normativa dell'UE in materia di protezione dei dati in tutti gli Stati membri e un'adeguata revisione della direttiva 95/46/CE: i principi generali rimangono validi, ma occorre adattare il quadro attuale affinché possa rispondere meglio alle sfide poste dalla rapida evoluzione delle nuove tecnologie e dalla crescente globalizzazione, garantire un livello uniforme di protezione delle persone in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati nel mercato interno. È necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese,

[6] Il 28 gennaio 2011 (giornata della protezione dei dati), la Commissione europea e il Consiglio d'Europa hanno co-organizzato una conferenza ad alto livello per discutere gli aspetti della riforma del quadro normativo dell'Unione così come la necessità di standard comuni per la protezione dei dati applicabili a livello mondiale. Il **Parlamento europe**o ha approvato, con risoluzione del 6 luglio 2011, una relazione a sostegno dell'impostazione adottata dalla Commissione per la riforma del quadro normativo in materia di protezione dei dati (**risoluzione** 2011/2025 (INI).

offra alla persona in tutti gli Stati membri il medesimo livello di diritti giuridicamente tutelati, definisca gli obblighi in capo ai responsabili del trattamento e degli incaricati del trattamento e assicuri un monitoraggio costante del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri.

La **proposta di regolamento COM (2012) 11** al **Capo I** ("Disposizioni generali"), definisce l'oggetto, i campi di applicazione materiale e territoriale del regolamento e definisce la terminologia, che riprende quella utilizzata nella direttiva 95/46/CE, e la integra con elementi aggiuntivi della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, quale modificata dalla direttiva 2009/136/CE[7]. In particolare, quando si definisce il "consenso dell'interessato" (art. 4), rispetto alla direttiva 95/46/CE, si specifica che esso deve essere "esplicito" e non può essere tacito o passivo.

Al **Capo II** (Principi) la proposta stabilisce i principi in materia di trattamento dei dati personali[8]. Tra i nuovi elementi aggiunti rispetto alla direttiva 95/46/CE si trovano il principio di trasparenza, la precisazione del principio di minimizzazione dei dati e l'introduzione di una responsabilità generale del responsabile del trattamento. I dati personali devono pertanto essere: a) trattati in modo lecito, equo e trasparente nei confronti dell'interessato; b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità; c) adeguati, pertinenti e limitati al minimo necessario rispetto alle finalità perseguite; i dati possono essere trattati solo se e nella misura in cui le finalità non siano conseguibili attraverso il trattamento di informazioni che non contengono dati personali; d) esatti e aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; f) trattati sotto la responsabilità del responsabile del trattamento, che assicura e comprova, per ciascuna operazione, la conformità alle disposizioni del presente regolamento. Vengono poi chiarite le condizioni alle quali il consenso è valido come base giuridica ai fini di un trattamento lecito e le ulteriori condizioni nel caso di minori. L'**art. 9** stabilisce il divieto generale, e le relative eccezioni, di trattamento di categorie particolari di dati personali che rivelino la razza, l'origine etnica, le opinioni politiche, la religione o le convinzioni personali, l'appartenenza sindacale, come pure i dati relativi alla salute e alla vita sessuale o a condanne penali o a connesse misure di sicurezza e i dati genetici (questi ultimi, non menzionati nella direttiva 95/46/CE).

Il **Capo III** è dedicato ai diritti dell'interessato: viene introdotto l'obbligo per i responsabili del trattamento di fornire informazioni trasparenti, comprensibili e facilmente accessibili (**art. 11**) e imposto al responsabile del trattamento di predisporre le procedure e i meccanismi che permettano all'interessato di esercitare i propri diritti, compresi i mezzi per introdurre le richieste per via elettronica/telematica, l'obbligo di rispondere entro un termine determinato e di motivare un eventuale rifiuto. Vengono precisati gli obblighi di informazione del responsabile del trattamento, tra cui informazioni quali il periodo di conservazione, il diritto di presentare reclamo, i trasferimenti internazionali e la fonte dei dati (**art. 14**), aggiuntive

---

[7] 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) e Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

[8] Per "trattamento" si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la memorizzazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la cancellazione o la distruzione" (art. 4).

rispetto a quanto previsto nella direttiva 95/46/CE. Sono mantenute le deroghe previste dalla direttiva 95/46/CE, per cui l'obbligo di informazione non si applica se la registrazione o la divulgazione dei dati sono espressamente previste per legge. Ciò può avvenire, ad esempio, nei procedimenti avviati dalle autorità per la concorrenza, da un'amministrazione fiscale o doganale o dai servizi di sicurezza sociale.

La proposta prevede il diritto di accesso ai propri dati personali, la comunicazione all'interessato del periodo di conservazione dei dati, dei diritti di rettifica e di cancellazione e del diritto di proporre reclamo e il diritto all'oblio e alla cancellazione prevedendo le condizioni del diritto all'oblio, compreso l'obbligo del responsabile del trattamento che abbia divulgato dati personali di informare i terzi della richiesta dell'interessato di cancellare tutti i link verso tali dati, le loro copie o riproduzioni (**art. 17**). L'**art. 18** introduce il diritto dell'interessato alla portabilità dei dati, vale a dire il diritto di trasferire i propri dati da un sistema di trattamento elettronico a un altro, senza che il responsabile del trattamento possa impedirlo. L'**art. 20** è dedicato alla profilazione: viene sancito il diritto di non essere sottoposto a misure basate sulla profilazione e si stabilisce che chiunque ha il diritto di non essere sottoposto a una misura che produca effetti giuridici o significativamente incida sulla sua persona, basata unicamente su un trattamento automatizzato destinato a valutare taluni aspetti della sua personalità o ad analizzarne o prevederne in particolare il rendimento professionale, la situazione economica, l'ubicazione, lo stato di salute, le preferenze personali, l'affidabilità o il comportamento.

L'**art**. **21** chiarisce la facoltà dell'Unione o degli Stati membri di mantenere o introdurre **limitazioni dei suddetti principi** per salvaguardare la pubblica sicurezza, le attività volte a prevenire, indagare, accertare e perseguire reati, altri interessi pubblici di natura economica e finanziaria dell'Unione o di uno Stato membro, la tutela dell'interessato o dei diritti e delle libertà altrui.

Al **Capo IV** vengono definiti dettagliatamente gli obblighi e i compiti del responsabile del trattamento dei dati e, qualora il trattamento non venga effettuato dal responsabile, dell'incaricato del trattamento, fin dalla progettazione ("*by design"*) e di *default*. L'**art**. **28** introduce l'obbligo per i responsabili e gli incaricati del trattamento di conservare la documentazione delle operazioni effettuate sotto la propria responsabilità, mentre gli obblighi di trattamento devono concentrarsi sulle sole operazioni di trattamento che presentano rischi particolari per le libertà dei soggetti interessati a differenza della notifica indiscriminata e generale all'autorità di controllo prevista dall'articolo 18, paragrafo 1, e dall'articolo 19 della direttiva 95/46/CE.

Viene inoltre introdotto l'obbligo di notificazione e comunicazione delle violazioni di dati personali (artt. 31 e 32)[9] e ne vengono chiarite le modalità.

Viene introdotta la figura obbligatoria del responsabile della protezione dei dati per l'intero settore pubblico e, nel settore privato, per le imprese con 250 o più dipendenti o allorquando le attività principali del responsabile del trattamento e dell'incaricato del trattamento consistano in trattamenti che richiedono il controllo regolare e sistematico degli interessati (**art. 35**)[10].

Gli Stati membri e la Commissione incoraggiano, in particolare a livello europeo, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi

[9] come previsto all'articolo 4, paragrafo 3, della direttiva 2002/58/CE (Direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[10] La disposizione si basa sull'articolo 18, paragrafo 2, della direttiva 95/46/CE che ha permesso agli Stati membri di introdurre tale obbligo in sostituzione di un obbligo generale di notificazione. La Commissione europea osserva che l'obbligo per gli operatori economici di grandi dimensioni (con più di 250 dipendenti) di designare un responsabile della protezione dei dati non genererebbe costi sproporzionati, in quanto tale figura è già comune in tali imprese. Tale obbligo si applicherà a una fascia minima necessaria di responsabili del trattamento, dato che di norma le PMI ne saranno escluse.

di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati garantito dai responsabili del trattamento e dagli incaricati del trattamento.

Il **Capo V** affronta e regola il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali. Il trasferimento verso un paese terzo o un'organizzazione internazionale, compreso il trasferimento successivo di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, è ammesso se la Commissione ha deciso che il paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato (**art. 41**). La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea l'elenco dei paesi terzi, dei territori e settori di trattamento all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è garantito un livello di protezione adeguato. In mancanza di una decisione di adeguatezza della Commissione, i trasferimenti a paesi terzi sono subordinati ad adeguate garanzie, in particolare clausole tipo di protezione dei dati, norme vincolanti d'impresa e clausole contrattuali. Vengono poi precisate le deroghe per il trasferimento di dati (i trasferimenti di dati richiesti e necessari per motivi di interesse pubblico rilevante, per esempio in casi di scambi internazionali di dati tra amministrazioni fiscali o doganali oppure tra servizi competenti per la sicurezza sociale, **art. 44**).

Il **Capo VI** è dedicato alle autorità di controllo indipendenti che gli Stati membri sono obbligati a istituire, come già previsto dalla direttiva 95/46/CE, incaricate di sorvegliare l'applicazione del presente regolamento e di contribuire alla sua coerente applicazione in tutta l'Unione. Vengono date disposizioni sull'istituzione e sulla nomina dei membri delle autorità. L'**art. 51** prevede che l'autorità di controllo abbia competenza nel territorio del suo Stato membro, come già previsto dalla direttiva 95/46/CE , ma viene introdotta la nuova competenza di autorità capofila nel caso di un responsabile del trattamento o incaricato del trattamento stabilito in più Stati membri, al fine di assicurare un'attuazione uniforme ("sportello unico")[11]. I tribunali, nell'esercizio della loro funzione giurisdizionale, sono esentati dal monitoraggio esercitato dall'autorità di controllo, ma non dall'applicazione delle norme sostanziali in materia di protezione dei dati. Vengono poi definite le funzioni e i poteri delle autorità. Viene ribadito l'obbligo di redigere relazioni annuali di attività, com'era già previsto dalla direttiva 95/46/CE.

Nal **Capo VII** si definiscono le norme esplicite con cui le autorità di controllo si trasmettono le informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il regolamento in maniera coerente e cooperare efficacemente tra loro[12]. Si specificano le conseguenze per la mancata esecuzione della richiesta di un'altra autorità di controllo. Si introduce inoltre un "meccanismo di coerenza" (**art. 57-61**) volto ad assicurare l'uniformità di applicazione in relazione alle attività di trattamento dati che possono riguardare interessati in vari Stati membri.

Viene istituito il comitato europeo per la protezione dei dati (**art. 64**), composto dal responsabile delle autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati. Ne vengono definiti i compiti. Il comitato europeo per la protezione dei dati sostituisce il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dalla direttiva 95/46/CE. La Commissione non è membro del comitato europeo per la protezione dei dati, ma ha il diritto di partecipare alle attività e designa un rappresentante.

---

[11] La Commissione osserva che la chiarificazione e la semplificazione delle norme attraverso la definizione di un'unica legge applicabile in tutta l'Unione e la creazione di uno "sportello unico" per il controllo della protezione dei dati rafforzeranno il mercato interno, in particolare grazie all'eliminazione delle divergenze tra le formalità amministrative a carico delle autorità di protezione dei dati. Solo in termini di onere amministrativo, ciò dovrebbe comportare un risparmio globale di circa 2,3 miliardi di euro all'anno.

[12] Il nuovo meccanismo di cooperazione e assistenza reciproca tra le autorità di protezione dei dati comporterà costi supplementari anche per le autorità nazionali di protezione dei dati e il garante europeo della protezione dei dati.

Il **Capo VIII** riconosce a ciascuno il diritto di presentare un reclamo presso un'autorità di controllo e specifica anche gli organismi, le organizzazioni o associazioni che possono presentare reclamo per conto dell'interessato o, in caso di violazione di dati personali, indipendentemente dal reclamo dell'interessato. Vengono poi regolati i ricorsi giurisdizionali contro il responsabile o l'incaricato del trattamento dei dati e contro l'autorità di controllo in modo da obbligare le autorità competenti a dare seguito a un reclamo in caso di mancata decisione nei tempi. Viene stabilito il diritto al risarcimento del danno causato dal responsabile del trattamento (**artt. 73-77**). Infine, gli Stati membri sono obbligati a definire le sanzioni applicabili alle violazioni del regolamento e di garantirne l'effettiva attuazione. Ciascuna autorità di controllo è obbligata a sanzionare gli illeciti amministrativi elencati, a comminare ammende entro un importo massimo, tenendo debitamente conto delle circostanze di ogni singolo caso (**art. 79**)[13].

Il **Capo IX** è dedicato a specifiche situazioni di trattamento dei dati. Innanzitutto gli Stati membri devono adottare esenzioni e deroghe alle disposizioni del regolamento ove necessario per conciliare il diritto alla protezione dei dati personali e il diritto alla libertà d'espressione[14]. Inoltre, in aggiunta a quanto già prescritto per categorie particolari di dati, vanno garantite specifiche salvaguardie al trattamento di dati a fini sanitari (**art. 81**) e nell'ambito dei rapporti di lavoro. Chiese e comunità religiose, alla luce dell'articolo 17 del TFUE[15], possono continuare ad applicare corpus completi di norme di protezione dei dati, purché conformi al regolamento (**art. 85**).

Il **Capo X** è dedicato all'adozione di atti delegati e di esecuzione. Al fine di conseguire gli obiettivi del regolamento, la proposta prevede (**art. 87**) che sia conferito alla Commissione il potere di adottare atti delegati a norma dell'articolo 290 del TFUE, al fine di definire,tra le altre cose, i criteri e le condizioni relativi al consenso dei minori; il trattamento di categorie particolari di dati; i criteri e le condizioni per le richieste manifestamente eccessive e il contributo spese per l'esercizio dei diritti dell'interessato; i criteri e i requisiti applicabili all'informazione dell'interessato e al diritto di accesso; il diritto all'oblio e alla cancellazione; le misure basate sulla profilazione; i criteri e requisiti per i trasferimenti in presenza di norme vincolanti d'impresa; le deroghe al trasferimento; le sanzioni amministrative; il trattamento a fini sanitari; il trattamento nel contesto del rapporto di lavoro e il trattamento per finalità storiche, statistiche e di ricerca scientifica.

Il **Capo XI** contiene le disposizioni finali: viene abrogata la direttiva 95/46/CE e viene chiarito il rapporto con la direttiva 2002/58/CE sulla vita privata e le comunicazioni elettroniche. Viene infine stabilita la data di entrata in vigore del regolamento e una fase transitoria rispetto alla data di applicazione.

Il quadro relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati si completa con la **proposta di direttiva in esame,** concernente il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati. La proposta è finalizzata a garantire un livello elevato e uniforme di protezione dei dati in questo settore, in modo da accrescere la fiducia reciproca tra

---

[13] L'articolo specifica poi tre livelli massimi per le sanzioni pecuniarie amministrative, a seconda del tipo di violazione (da 250.000 a un milione di euro, e per le imprese, dallo 0,5% al 2% del fatturato mondiale annuo).

[14] Come interpretato dalla Corte di giustizia europea. Si veda ad esempio la causa C-73/07: sentenza della Corte di giustizia dell'Unione europea 16 dicembre 2008 - Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy, Satamedia Oy, Racc. 2008 pag. I-9831.

[15] "1. L'Unione rispetta e non pregiudica lo status di cui le chiese e le associazioni o comunità religiose godono negli Stati membri in virtù del diritto nazionale. 2. L'Unione rispetta ugualmente lo status di cui godono, in virtù del diritto nazionale, le organizzazioni filosofiche e non confessionali. 3. Riconoscendone l'identità e il contributo specifico, l'Unione mantiene un dialogo aperto, trasparente e regolare con tali chiese e organizzazioni".

le autorità di polizia e giudiziarie di diversi Stati membri e agevolare la libera circolazione dei dati e la cooperazione tra i servizi di polizia e le autorità giudiziarie.

Una direttiva è lo strumento migliore per garantire l'armonizzazione a livello dell'UE in tale settore e per offrire al tempo stesso la flessibilità necessaria agli Stati membri quando attuano i principi, le norme e le rispettive esenzioni a livello nazionale. In vista dell'obiettivo generale di armonizzare tali norme con la presente direttiva, la Commissione dovrà chiedere agli Stati membri di fornirle documenti esplicativi sui rapporti fra gli elementi della direttiva e le corrispondenti parti degli strumenti nazionali di attuazione affinché possa adempiere ai propri compiti controllando l'attuazione della presente direttiva.

Disposizioni specifiche per la protezione dei dati personali nei settori della cooperazione giudiziaria e di polizia in materia penale sono contenute nella decisione quadro 2008/977/GAI, che la proposta in esame va ad abrogare. Tale decisione ha un campo di applicazione limitato al trattamento transfrontaliero dei dati e non alle attività di trattamento effettuate dalla polizia e dalle autorità giudiziarie a livello strettamente nazionale, creando difficoltà per le forze di polizia e le altre autorità competenti nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia per le quali può non essere sempre agevole stabilire il carattere puramente nazionale o transfrontaliero di un trattamento di dati o prevedere se i dati "nazionali" possano essere oggetto di un successivo scambio transfrontaliero. Inoltre, per sua natura e contenuto, la decisione quadro lascia un ampio margine di manovra alle legislazioni nazionali degli Stati membri nell'attuazione delle sue disposizioni e non conferisce competenze di esecuzione alla Commissione per garantire un approccio attuativo comune.

Nel dettaglio, al **Capo I**, vengono definiti l'oggetto della direttiva, gli obiettivi (tutelare il diritto alla protezione dei dati personali, garantendo nel contempo un elevato livello di sicurezza pubblica, e garantire lo scambio dei dati personali tra le autorità competenti all'interno dell'Unione), il campo di applicazione (la direttiva non si applica al trattamento di dati nel corso di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione). Vengono poi definiti i principi relativi al trattamento dei dati personali.

Quanto ai principi, contenuti nel **Capo II**, gli **articoli 5 e 6** prevedono che gli Stati membri dispongano che, nella misura del possibile, il responsabile del trattamento operi una chiara distinzione tra i dati personali di diverse categorie di interessati, quali le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato; le persone condannate per un reato; le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato; i terzi coinvolti nel reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati; le persone che non rientrano in nessuna delle precedenti categorie. Inoltre gli Stati membri devono provvedere affinché, nella misura del possibile, sia effettuata una distinzione tra diverse categorie di dati personali oggetto di trattamento in base al loro grado di esattezza e affidabilità e che i dati personali fondati su fatti siano differenziati da quelli fondati su valutazioni personali[16].

L'**art. 7** chiarisce che il trattamento è lecito quando è necessario per l'esecuzione di un compito di un'autorità competente in base al diritto nazionale, per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, per proteggere gli interessi vitali dell'interessato o di un terzo o per prevenire un'immediata e grave minaccia alla sicurezza pubblica.

[16] Come previsto dalla raccomandazione del Consiglio d'Europa n. R (87) 15: Principio n. 3.1. Nella misura del possibile, la registrazione di dati a carattere personale a fini di polizia non dovrà riguardare che alcuni dati specifici e dovrà limitarsi ai dati necessari per consentire agli organi di polizia di svolgere i loro compiti legali in un quadro di diritto interno e di obbligazioni derivanti dal diritto internazionale; Principio n. 3.2. Per quanto possibile, dovranno essere differenziate le differenti categorie di dati registrati, in funzione del loro grado di esattezza o di affidabilità ed, in particolare, i dati fondati su fatti dovranno essere differenziati da quelli fondati su opinioni o valutazioni personali.

L'**art.8** prevede che gli Stati membri vietino il trattamento di dati personali che rivelino la razza, l'origine etnica, le opinioni politiche, la religione o le convinzioni personali, l'appartenenza sindacale, come pure il trattamento di dati genetici o dati relativi alla salute e alla vita sessuale, tranne quando il trattamento è autorizzato da disposizioni di legge che prevedono garanzie adeguate, oppure il trattamento è necessario per salvaguardare un interesse vitale dell'interessato o di un terzo, oppure il trattamento riguarda dati resi manifestamente pubblici dall'interessato.

Nel **Capo III** vengono affrontati i diritti dell'interessato: gli Stati membri devono disporre che il responsabile del trattamento fornisca all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile[17]. Sono previste deroghe all'obbligo di informazione, quando costituiscano misure necessarie e proporzionate in una società democratica per l'adempimento dei compiti delle autorità competenti[18]. L'interessato ha il diritto di chiedere che l'autorità di controllo verifichi la liceità del trattamento e che venga informato quanto meno dell'avvenuto espletamento di tutte le verifiche necessarie e del loro esito riguardo alla liceità del trattamento in questione. L'interessato ha il diritto di ottenere dal responsabile del trattamento la rettifica di dati personali inesatti e la cancellazione di dati personali nel caso il trattamento non sia lecito[19]. Il responsabile del trattamento provvede alla cancellazione oppure contrassegna i dati personali quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche; quando i dati personali devono essere conservati a fini probatori; quando l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo. Nella proposta si parla di "contrassegnare", eliminando l'ambiguità del termine "bloccare" usato nell'articolo 4, paragrafo 4, comma 3, della decisione quadro 2008/977/GAI[20].

Al **Capo IV** vengono chiarite le politiche e le misure che il responsabile del trattamento deve adottare per garantire che il trattamento effettuato sia conforme a quanto prevede la proposta di direttiva. Vengono chiarite le responsabilità di eventuali figure che intervengono per conto del responsabile (incaricati, corresponsabili) e viene regolata la cooperazione con l'autorità di controllo nell'esercizio delle sue funzioni.

Quanto alla sicurezza dei dati, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, il responsabile del trattamento e l'incaricato del trattamento sono obbligati a mettere

---

[17] All'interessato devono essere fornite almeno le seguenti informazioni: "a) l'identità e le coordinate di contatto del responsabile del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento cui sono destinati i dati personali; c) il periodo per il quale i dati personali saranno conservati; d) l'esistenza del diritto dell'interessato di chiedere al responsabile del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali che lo riguardano o la limitazione di trattamento; e) il diritto di proporre reclamo all'autorità di controllo di cui all'articolo 39 e le coordinate di contatto di detta autorità; f) i destinatari o le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali; g) ogni altra informazione necessaria per garantire un trattamento equo nei confronti dell'interessato, in considerazione delle specifiche circostanze in cui i dati personali vengono trattati" (Art. 11).

[18] Cfr. l'articolo 17.2 della decisione quadro 2008/977/GAI: a) per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) per non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento dei reati o per l'esecuzione delle sanzioni penali; c) per proteggere la sicurezza pubblica; d) per proteggere la sicurezza dello Stato; e) per proteggere la persona interessata o i diritti e le libertà altrui.

[19] Art. 18.1della decisione quadro 2008/977/GAI : "La persona interessata ha diritto a che il responsabile del trattamento adempia i propri obblighi riguardanti la rettifica, la cancellazione o il blocco dei dati personali che gli incombono in virtù della presente decisione quadro. Gli Stati membri stabiliscono se la persona interessata possa far valere questo diritto contro il responsabile del trattamento direttamente o tramite l'autorità nazionale di controllo competente. Se il responsabile del trattamento rifiuta la rettifica, la cancellazione o il blocco, il rifiuto deve essere comunicato per iscritto alla persona interessata, che deve essere informata circa i mezzi previsti dalla legislazione nazionale per presentare un reclamo o un ricorso. In fase di esame del reclamo o del ricorso, la persona interessata è informata della correttezza o meno dell'agire del responsabile del trattamento. Gli Stati membri possono inoltre disporre che la persona interessata sia informata dall'autorità nazionale di controllo competente che si è proceduto a un esame".

[20] "I dati personali non vengono cancellati ma solo bloccati se vi sono motivi ragionevoli di ritenere che la cancellazione possa compromettere gli interessi legittimi della persona interessata. I dati bloccati sono trattati solo per lo scopo che ha impedito la loro cancellazione".

in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta e alla natura dei dati personali da proteggere. Vengono poi elencate le misure da adottare da parte del responsabile del trattamento in caso di violazione dei dati personali (tempi e modalità della notifica all'autorità di controllo e all'interessato). Viene inoltre prevista la designazione di un responsabile della protezione dei dati da parte del responsabile del trattamento, e ne vengono definiti i compiti.

Il **Capo V** è dedicato al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali. L'**articolo 33** stabilisce i principi generali per il trasferimento di dati nel settore della cooperazione di polizia e giudiziaria in materia penale, compresi i trasferimenti successivi. e precisa che i trasferimenti di dati verso i paesi terzi sono ammessi solo se necessari a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. L'**articolo 34** stabilisce che i trasferimenti verso un paese terzo sono ammessi solo se la Commissione ha adottato una decisione di adeguatezza, conformemente a quanto previsto nella proposta di regolamento già esaminata, nei confronti di tale paese terzo, o se ciò avviene specificamente nell'ambito della cooperazione di polizia o giudiziaria in materia penale, o, in mancanza di tale decisione, se sono state poste in essere adeguate garanzie. Nelle more di una decisione di adeguatezza, la direttiva garantisce che i trasferimenti possano continuare sulla base di deroghe e in presenza di adeguate garanzie.

L'**articolo 38** prevede espressamente lo sviluppo di meccanismi di cooperazione internazionale per la protezione dei dati personali tra la Commissione e le autorità di controllo di paesi terzi, in particolare quelli che si ritiene offrano un adeguato livello di protezione[21].

Al **Capo VI**, l'**art. 39** obbliga gli Stati membri a istituire una o più autorità di controllo affinché possano contribuire alla coerente applicazione della direttiva in tutta l'Unione[22]; tale autorità può essere la stessa prevista nella proposta di regolamento generale sulla protezione dei dati. Ne vengono chiariti competenze, funzioni e poteri (**artt. 44-47**). Tra le funzioni dell'autorità di controllo è compresa quella di ricevere ed esaminare i reclami o sensibilizzare il pubblico ai rischi, alle norme e misure di salvaguardia e ai diritti. Una particolare funzione dell'autorità di controllo consiste nell'esercitare il diritto di accesso per conto dell'interessato, qualora l'accesso diretto sia negato o limitato, e verificare la liceità del trattamento dei dati.

Nel **Capo VII** viene introdotto l'obbligo di assistenza reciproca tra le autorità di controllo e vengono chiariti i compiti del comitato europeo per la protezione dei dati previsto dalla proposta di regolamento in merito ai trattamenti rientranti nel campo di applicazione della proposta di direttiva in oggetto.

Il **Capo VIII** regola il diritto di presentare un reclamo presso un'autorità di controllo di qualunque Stato membro e riprende quanto previsto nella proposta di regolamento.

Il **Capo IX** è dedicato all'adozione di atti delegati e di esecuzione, mentre il **Capo X** contiene le disposizioni finali: viene abrogata la decisione quadro 2008/977GAI, rimangono impregiudicate le disposizioni specifiche per la protezione dei dati personali con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, contenute in atti dell'Unione adottati prima della data di adozione della presente direttiva. L'**art. 60** chiarisce il rapporto della presente direttiva con accordi internazionali conclusi precedentemente dagli Stati membri nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia. L'articolo 61 dispone che la Commissione deve valutare lo stato di attuazione della direttiva e redigere apposite relazioni, al fine di valutare la necessità di allineare alla presente

[21] Si rimanda alla raccomandazione dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) sulla cooperazione transfrontaliera nell'applicazione delle legislazioni in materia di privacy del 12 giugno 2007.

[22] come già previsto dall'articolo 28, paragrafo 1, della direttiva 95/46/CE e dall'articolo 25 della decisione quadro 2008/977/GAI.

direttiva le specifiche disposizioni adottate precedentemente, di cui all'**art. 59**. L'**art. 62** stabilisce l'obbligo degli Stati membri di recepire la direttiva nel diritto nazionale e comunicare alla Commissione le disposizioni adottate in applicazione della direttiva.

Le specifiche **implicazioni di bilancio** della proposta riguardano i compiti assegnati al garante europeo della protezione dei dati. Tali implicazioni richiedono una riprogrammazione della rubrica delle prospettive finanziarie.

Conformemente alla ripartizione dei compiti, risorse dovranno essere fornite alla Commissione e dal garante europeo della protezione dei dati. Per quanto riguarda la Commissione, le risorse necessarie sono già comprese nelle prospettive finanziarie per il periodo 2014-2020. La protezione dei dati è uno degli obiettivi del programma Diritti e cittadinanza, che sosterrà anche alcune misure per realizzare il quadro normativo. Gli stanziamenti amministrativi, che comprendono il fabbisogno di personale, sono inclusi nel bilancio amministrativo della DG JUST.

Per quanto concerne il garante europeo della protezione dei dati, le risorse necessarie dovranno essere prese in considerazione nei rispettivi bilanci annuali che lo riguardano. Le risorse sono specificate nel dettaglio nella scheda finanziaria. Al fine di fornire le risorse necessarie per i nuovi compiti del comitato europeo per la protezione dei dati, le cui funzioni di segreteria saranno espletate dal garante europeo della protezione dei dati, sarà necessaria una riprogrammazione della rubrica 5 delle prospettive finanziarie 2014-2020.

Va ricordato che il 7 marzo 2012, il **Garante europeo per la protezione dei dati** ha sottolineato come la normativa proposta dalla Commissione non realizzi l'auspicato approccio globale al tema, anche a causa della diversità degli strumenti giuridici utilizzati[23]. In particolare, pur condividendo la scelta dello strumento del regolamento per la normativa generale in materia di protezione dei dati, il Garante esprime alcune riserve in relazione alle possibilità di restrizione dei principi e dei diritti di base; alle deroghe possibili nel quadro dei trasferimenti di dati ai paesi terzi; ai poteri, giudicati eccessivi, accordati alla Commissione europea nel meccanismo di coerenza; alle nuove eccezioni al principio di limitazione della finalità. Per quanto riguarda la proposta di direttiva, il Garante europeo ritiene che le regole per la protezione dei dati in materia penale siano troppo deboli e abbassino il livello di protezione come definito nella proposta di regolamento generale. Il Garante esprime in particolare preoccupazione per: la mancanza di certezza giuridica per quanto riguarda l'utilizzazione ulteriore dei dati a carattere personale da parte delle autorità di polizia e giudiziarie; l'assenza di un obbligo generale per le autorità giudiziarie e di polizia di dimostrare la conformità con le esigenze di protezione dei dati; le condizioni insufficienti per il trasferimento verso paesi terzi; i poteri limitati delle autorità di controllo.

Si fa presente che il **Senato francese**, in merito alla proposta di regolamento, ha adottato un **parere motivato** per violazione del principio di sussidiarietà. Tra le motivazioni è citata la norma relativa allo "sportello unico" (art.51) che priverebbe gli interessati della possibilità di rivolgersi all'autorità di controllo nazionale dello Stato membro in cui risiedono e produrrebbe situazioni estremamente complesse in ragione della asimmetria tra i ricorsi amministrativi presentati presso l'autorità di controllo straniera e i ricorsi giurisdizionali contro il responsabile del trattamento presentati presso il giudice nazionale. Inoltre, si sottolinea che l'elevato numero di deleghe conferite alla Commissione europea (art. 87) sembrerebbe andare al di là della natura stessa degli atti delegati come definita nell'articolo 290 TFUE. Il diritto all'oblio, ad esempio, dovrebbe essere regolato direttamente dal legislatore europeo. Gli oggetti di alcune deleghe potrebbero rientrare più correttamente nella competenza delle autorità di controllo nazionali o nei loro raggruppamenti a livello europeo.

[23] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-07_DPReform_package_EN.pdf

Inoltre, il Bundesrat tedesco e il Parlamento svedese hanno annunciato che si esprimeranno sulla sussidiarietà con parere motivato, mentre il Parlamento spagnolo, pur considerando le proposte in oggetto conformi, raccomanda che venga chiaramente definito il concetto di "sicurezza nazionale" per evitare qualsiasi ambiguità.

---

28 marzo 2012
A cura di Vitaliana Curigliano
Per informazioni: Ufficio dei rapporti con le istituzioni dell'Unione europea (roci01a@senato.it)