00062/10/IT
WP 173

Parere 3/2010 sul principio di responsabilità

adottato il 13 luglio 2010

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

SINTESI

I principi e gli obblighi dell'Unione europea in materia di protezione dei dati sono spesso applicati in modo insufficiente a livello di misure e pratiche interne sostanziali. Se la protezione dei dati non diventa parte integrante delle pratiche e dei valori condivisi di un'organizzazione e se le relative responsabilità non sono espressamente ripartite, il rispetto effettivo delle norme in materia di protezione dei dati sarà messo notevolmente a rischio e gli incidenti in questo settore saranno destinati a continuare.

Per favorire l'attuazione della protezione dei dati nella pratica, il quadro normativo dell'Unione europea necessita di strumenti aggiuntivi. Il presente parere intende consigliare la Commissione su come modificare in tal senso la direttiva sulla protezione dei dati. In particolare, questo parere avanza una proposta concreta per l'introduzione di un principio di responsabilità che richieda ai responsabili del trattamento di mettere in atto misure adeguate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati e per dimostrare tale osservanza, su richiesta, alle autorità di controllo. Ciò dovrebbe contribuire a passare "dalla teoria alla pratica" e ad aiutare le autorità di protezione dei dati nello svolgimento dei loro compiti di controllo e di verifica dell'applicazione.

Il parere contiene suggerimenti volti ad assicurare che il principio di responsabilità garantisca la certezza del diritto, lasciando spazio al tempo stesso ad una certa adattabilità (che consenta di determinare le misure concrete da applicare in funzione dei rischi connessi al trattamento e dei tipi di dati trattati). Si analizza quindi in che modo tale principio potrebbe ripercuotersi in altri settori, tra i quali i trasferimenti internazionali di dati, gli obblighi di notificazione, le sanzioni e, infine, anche lo sviluppo di programmi o sigilli di certificazione.

Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti l'articolo 29, l'articolo 30, paragrafo 1, lettera a), e l'articolo 30, paragrafo 3, della suddetta direttiva e l'articolo 15, paragrafo 3, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 giugno 2002,

visto il proprio regolamento interno,

ha adottato il seguente parere:

1. INTRODUZIONE

1. La protezione dei dati deve passare "dalla teoria alla pratica". Gli obblighi giuridici devono essere tradotti in misure concrete di protezione dei dati. Per favorire la protezione dei dati nella pratica, il quadro giuridico dell'UE in materia necessita di meccanismi aggiuntivi. Nei dibattiti sul futuro del quadro europeo e globale sulla protezione dei dati, sono stati proposti meccanismi basati sulla responsabilità come mezzo per incoraggiare i responsabili del trattamento ad attuare strumenti pratici per una protezione dei dati efficace.

2. Nel suo documento sul futuro della privacy (WP168) del dicembre 2009, il Gruppo di lavoro articolo 29 ha ritenuto che l'attuale quadro giuridico non sia riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si traducano in meccanismi efficaci atti a fornire una protezione reale. Per migliorare la situazione, il Gruppo di lavoro ha proposto che la Commissione esamini l'opportunità di introdurre meccanismi basati sulla responsabilità, con un particolare accento sulla possibilità di includere un principio di "responsabilità" nella versione riveduta della direttiva sulla protezione dei dati[1]. Tale principio rafforzerebbe il ruolo del responsabile del trattamento e ne aumenterebbe la responsabilità.

3. In breve, un principio di responsabilità vincolante imporrebbe esplicitamente ai responsabili del trattamento di attuare misure appropriate ed efficaci per dare

[1] "Per risolvere questo problema, sarebbe opportuno introdurre nel quadro globale un principio di responsabilità in base al quale i responsabili del trattamento dei dati siano tenuti ad adottare le misure necessarie per garantire il rispetto degli obblighi e dei principi fondamentali dell'attuale direttiva al momento del trattamento dei dati personali. Una disposizione di questo tipo rafforzerebbe la necessità di mettere in atto politiche e meccanismi per l'attuazione efficace dei principi e degli obblighi fondamentali della direttiva attuale. Avrebbe inoltre l'obiettivo di confermare l'esigenza di adottare misure adeguate che determinino un'efficace applicazione interna degli obblighi e dei principi fondamentali attualmente stabiliti dalla direttiva. Inoltre, il principio della responsabilità imporrebbe ai responsabili del trattamento dei dati di disporre dei meccanismi interni necessari per dimostrarne la conformità agli interessati esterni, comprese le autorità nazionali di protezione dei dati. Infine, il fatto di dover dimostrare che sono state adottate misure adeguate per garantire la conformità favorirà notevolmente l'applicazione delle norme vigenti" (WP168, punto 79. Per maggiori informazioni, v. anche punti 74-78).

applicazione ai principi e agli obblighi della direttiva, e per dimostrarne su richiesta l'osservanza. In pratica, ciò dovrebbe concretarsi in programmi improntati all'adattabilità mirati ad attuare i principi esistenti di protezione dei dati (talvolta denominati "programmi di conformità"). Quale complemento a tale principio, potrebbero essere istituiti obblighi aggiuntivi diretti ad attuare garanzie di protezione dei dati o ad assicurarne l'efficacia. Potrebbe trattarsi, per esempio, di una disposizione che obbliga a effettuare una valutazione d'impatto sulla privacy per le operazioni di trattamento di dati a più alto rischio.

4. Il presente parere intende sviluppare il precedente contributo fornito sull'argomento dal Gruppo di lavoro articolo 29 con il parere sul futuro della privacy, allo scopo di assistere la Commissione nella revisione della direttiva 95/46, attualmente in corso. A tal fine, il presente parere è suddiviso in quattro sezioni: la prima esamina la necessità che i responsabili del trattamento rafforzino le prassi interne (politiche e procedure) per garantire che la totalità del trattamento avvenga in base alle norme vigenti, e spiega in che modo i sistemi basati sulla responsabilità possono contribuire a questo obiettivo. Prospetta quindi la forma che l'architettura giuridica di un sistema basato sulla responsabilità potrebbe assumere e i precedenti nel settore della protezione dei dati e in altri settori. La seconda sezione presenta una proposta concreta per un principio di responsabilità e descrive la logica alla base dei diversi aspetti della proposta. La terza sezione illustra vari elementi collegati ad un sistema giuridico che integri un sistema generale di responsabilità. Comprende un'analisi della necessità che tale proposta fornisca certezza giuridica e che sia al tempo stesso formulata in termini sufficientemente ampi da consentire una certa adattabilità (in modo da permettere di determinare le misure concrete e i metodi di verifica da applicare in funzione del rischio del trattamento e del tipo di dati trattati). Affronta quindi taluni elementi correlati, come ad esempio il rapporto con i trasferimenti all'estero, descrive i vantaggi che un meccanismo basato sulla responsabilità offrirebbe alle autorità di protezione dei dati e delinea il ruolo che potrebbe svolgere la certificazione.

II. RESPONSABILITÀ: OBIETTIVI, ARCHITETTURA GIURIDICA, PRECEDENTI E TERMINOLOGIA

II.1 Responsabilità come motore per l'attuazione efficace dei principi di protezione dei dati

5. Oggi si rivela sempre più necessario e importante che i responsabili del trattamento adottino misure efficaci per una reale protezione dei dati. Le ragioni sono molteplici e vengono analizzate nel prosieguo.

6. Anzitutto, rispetto ai dati stiamo assistendo ad un cosiddetto "effetto diluvio" , con un continuo aumento della quantità di dati personali esistenti, elaborati e ulteriormente trasferiti. Questo fenomeno è favorito sia dai progressi tecnologici, vale a dire lo sviluppo dei sistemi di informazione e di comunicazione, sia dalla crescente capacità degli utenti di impiegare le tecnologie e interagire con esse. Con l'aumento della quantità di dati trasferiti in tutto il mondo, aumentano anche i rischi di abuso. Ciò evidenzia ulteriormente la necessità che i responsabili del

trattamento, sia nel settore pubblico che in quello privato, attuino meccanismi interni reali ed efficaci per salvaguardare la tutela delle informazioni personali.

7. In secondo luogo, la quantità sempre crescente di dati personali è accompagnata da un aumento del loro valore in termini sociali, politici ed economici. In alcuni settori, soprattutto in ambiente online, i dati personali sono diventati *de facto* la valuta di scambio per i contenuti online. Nel contempo, da un punto di vista sociale, vi è un crescente riconoscimento della protezione dei dati come valore sociale. In sintesi, via via che i dati personali diventano sempre più preziosi per i responsabili del trattamento in tutti i settori, anche i cittadini, i consumatori e la società in generale sono sempre più consapevoli della loro rilevanza. Questo fatto rafforza a sua volta la necessità di applicare misure rigorose per salvaguardarli.

8. Infine, da quanto precede consegue che la violazione della privacy può avere notevoli ripercussioni negative per i responsabili del trattamento nei settori pubblico e privato. Potenziali anomalie nelle applicazioni di governo elettronico e di sanità elettronica avranno conseguenze devastanti sia in termini economici sia, soprattutto, in termini di reputazione. Pertanto, ridurre al minimo i rischi, costruire e mantenere una buona reputazione e garantire la fiducia dei cittadini e dei consumatori stanno diventando compiti fondamentali dei responsabili del trattamento in tutti i settori.

9. In sintesi, da quanto precede emerge l'assoluta necessità per i responsabili del trattamento di applicare misure reali ed efficaci di protezione dei dati dirette alla corretta gestione della loro protezione, riducendo inoltre al minimo i rischi giuridici, economici e di reputazione che possono derivare da pratiche inadeguate in materia. Come ulteriormente illustrato nel prosieguo, i meccanismi basati sulla responsabilità mirano a realizzare tali obiettivi.

II.2 Possibile architettura giuridica generale dei meccanismi basati sulla responsabilità

10. In questo contesto, una questione pertinente da chiarire riguarda il modo in cui il quadro giuridico potrebbe incoraggiare i responsabili del trattamento ad adottare misure che offrano una protezione reale nella pratica. In altri termini, la forma che dovrebbe assumere l'architettura giuridica dei sistemi basati sulla responsabilità.

11. In via preliminare, prima di analizzare tale architettura, occorre sottolineare che tali sistemi non modificano né influiscono in alcun modo sui principi sostanziali di protezione dei dati, bensì sono intesi a farli funzionare meglio.

12. Un modo per indurre i responsabili del trattamento a predisporre tali misure sarebbe inserire un principio di responsabilità nella versione riveduta della direttiva. Si prevede che una disposizione di questo tipo possa condurre all'attuazione di misure e procedure interne volte a rendere effettivi i principi di protezione dei dati esistenti assicurandone l'efficacia, e ad introdurre l'obbligo di dimostrarne il rispetto qualora le autorità di protezione dei dati ne facciano richiesta. Come ulteriormente descritto di seguito, il tipo di procedure e di meccanismi varierebbe in funzione dei rischi intrinseci al trattamento e alla natura dei dati.

13. In aggiunta a quanto precede, si potrebbe svolgere una riflessione su disposizioni specifiche quali l'obbligo di effettuare valutazioni d'impatto sulla privacy in determinati casi o la nomina di responsabili della protezione dei dati. Tali disposizioni specifiche potrebbero completare il principio generale di responsabilità.

14. Il Gruppo di lavoro articolo 29 riconosce che i responsabili del trattamento potrebbero avere la volontà di attuare politiche e procedure non strettamente previste dalla legislazione sulla protezione dei dati. Ad esempio, un responsabile del trattamento potrebbe volersi impegnare a rispondere alle richieste di accesso entro un periodo di tempo molto breve, anche se la legge prevede una certa flessibilità. Potrebbe anche volersi impegnare a rispondere contemporaneamente alle richieste di accesso sia on-line che off-line, per assicurare la ricezione tempestivo ed efficace di tali informazioni. Si potrebbero anche immaginare situazioni in cui il responsabile del trattamento desideri offrire una tutela più ampia di quella garantita dalle disposizioni minime previste dal quadro giuridico generale. Ad esempio, il responsabile del trattamento potrebbe decidere di nominare un responsabile della protezione dei dati anche se la legge vigente non dispone un obbligo in tal senso. Ancora, il responsabile del trattamento potrebbe voler affidare a terzi l'incarico di eseguire un audit relativo a *tutte* le sue operazioni di trattamento dei dati, al fine di valutarne la conformità con il quadro giuridico in materia di protezione dei dati. Il Gruppo di lavoro apprezza queste iniziative e incoraggia il nuovo quadro giuridico di protezione dei dati a fornire incentivi affinché i responsabili del trattamento si orientino in tale direzione.

15. Conformemente a quanto precede, l'architettura giuridica dei meccanismi di responsabilità prevedrebbe due livelli: il primo livello sarebbe costituito da un obbligo di base vincolante per *tutti* i responsabili del trattamento. Tale obbligo comprenderebbe due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove. Questo primo livello potrebbe essere integrato da disposizioni specifiche. Il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure (norme di attuazione eccedenti il livello minimo). Pur riconoscendo l'importanza e i benefici di tali sistemi, il presente parere si occupa per lo più dell'obbligo di primo livello, in particolare del principio generale di responsabilità.

II.3 Principio della responsabilità nel settore della protezione dei dati e in altri settori e terminologia

Precedenti

16. Il Gruppo di lavoro articolo 29 osserva che il principio di responsabilità non è una novità in sé. Il suo espresso riconoscimento è ravvisabile nelle linee guida per la protezione della vita privata dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) adottati nel 1980. Il principio di responsabilità ivi contenuto

enuncia: “Il responsabile del trattamento dei dati dovrebbe essere responsabile del rispetto delle misure che rendono effettivi i principi indicati sopra”.

17. Di recente tale principio è stato inserito esplicitamente tra gli standard internazionali di Madrid, elaborati dalla Conferenza internazionale sulla protezione dei dati e la privacy[2]. È inoltre accolto nel più recente progetto di norma ISO 29100 che stabilisce un quadro per la privacy, ed è uno dei principali concetti del quadro giuridico sulla privacy sviluppato dall’APEC e delle sue norme sulla privacy transfrontaliera[3].

18. Da un punto di vista “statutario”, il Gruppo di lavoro articolo 29 rileva che i principi canadesi di informazione equa contenuti nella legge "Personal Information Protection And Electronic Documents Act" fanno riferimento alla responsabilità. Tra gli altri, il primo principio richiede lo sviluppo e l’attuazione di politiche e pratiche atte a garantire il rispetto dei dieci principi di informazione equa tra cui procedure per la protezione dei dati personali e per ricevere e rispondere a reclami e richieste di informazioni.

19. In aggiunta a quanto sopra, il Gruppo di lavoro articolo 29 rileva che le regole d’impresa vincolanti, utilizzate nel contesto dei trasferimenti internazionali di dati, riflettono il principio di responsabilità. Tra le regole d’impresa vincolanti si annoverano i codici di condotta elaborati e seguiti da organizzazioni multinazionali, contenenti misure interne intese a dare applicazione ai principi di protezione dei dati (ad esempio audit, programmi di formazione, reti di incaricati della privacy, sistemi di gestione dei reclami). Una volta esaminate dalle autorità nazionali di protezione dei dati, le regole d’impresa vincolanti sono considerate idonee a garantire un livello di protezione adeguato in relazione a un trasferimento o a una categoria di trasferimenti di dati personali tra le imprese che fanno parte dello stesso gruppo e che sono vincolate da tali regole ai sensi dell'articolo 25 e dell'articolo 26, paragrafo 2, della direttiva 95/46.

20. Al di fuori dell'ambito della protezione dei dati, vi sono alcuni esempi di responsabilità: tra questi, un programma che specifica le politiche e le procedure che un responsabile del trattamento deve seguire per garantire la conformità con leggi e regolamenti. Per esempio, i programmi di conformità sono obbligatori ai sensi dei regolamenti in materia di servizi finanziari. In altri casi, i programmi di conformità non sono obbligatori, ma vengono incoraggiati, come ad esempio nel settore delle regole in materia di concorrenza. In Canada per esempio, il commissario per la concorrenza ha sviluppato politiche elaborate relative ai programmi di conformità aziendale. La decisione delle aziende di applicare o meno un programma è facoltativa. Tuttavia, il commissario canadese per la concorrenza sottolinea l’importanza della conformità come strumento di

---

2 La persona responsabile deve: “a. adottare tutte le misure necessarie per rispettare i principi e gli obblighi istituiti dal presente documento e dalla normativa nazionale vigente e b. predisporre i meccanismi interni necessari per dimostrare tale conformità sia agli interessati sia alle autorità di controllo nell’esercizio dei loro poteri, come stabilito alla sezione 23”.

3 Oltre a quanto sopra esposto, il Centre for Information Policy Leadership è impegnato in un’iniziativa tesa a esplorare gli effetti del principio di responsabilità per quanto riguarda la protezione dei dati e la privacy. Cfr il sito www.informationpolicycentre.com

mitigazione del rischio ed evidenziai benefici giuridici, economici e in termini di reputazione[4].

Terminologia

21. Il termine inglese "accountability" (responsabilità) proviene dal mondo anglosassone, dove è di uso comune e dove il suo significato è ampiamente compreso e condiviso. Ciononostante, risulta complesso definire che cosa esattamente significhi "accountability" in pratica. In generale, comunque, l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e 'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente.

22. Nella maggior parte delle altre lingue europee, principalmente a causa delle differenze tra i sistemi giuridici, il termine "accountability" non è facilmente traducibile. Di conseguenza, il rischio di un'interpretazione variabile del termine, e quindi di una mancanza di armonizzazione, è sostanziale. Altri termini che sono stati suggeriti per rendere il senso di "accountability" sono: "reinforced responsibility" (responsabilità rafforzata), "assurance" (assicurazione), "reliability" (affidabilità), "trustworthiness" (attendibilità) e, in francese, "obligation de rendre des comptes" (obbligo di rendere conto) ecc. Si potrebbe altresì inferire che "accountability" si riferisce alla "attuazione dei principi relativi alla protezione dei dati".

23. Il presente documento si occupa quindi delle misure che dovrebbero essere adottate o previste per garantire la conformità nel settore della protezione dei dati. I riferimenti alla responsabilità devono pertanto essere intesi nel senso utilizzato nel presente parere, fatta salva la possibilità di trovare un'altra formulazione che meglio rispecchi il concetto qui esposto. È per questo che il documento non è incentrato sui termini, ma si concentra pragmaticamente sulle misure da adottare, piuttosto che sul concetto in sé.

III. VERSO UNA PROPOSTA PER UNA DISPOSIZIONE GENERALE SULLA RESPONSABILITÀ

III.1 Una disposizione generale per riaffermare e rafforzare la responsabilità dei responsabili del trattamento

24. Il Gruppo di lavoro articolo 29 ha esaminato ulteriormente la possibilità di introdurre soluzioni basate sulla responsabilità nel nuovo quadro giuridico globale sulla protezione dei dati alla luce delle considerazioni esposte nella sezione I.

25. Di conseguenza, ha confermato il punto di vista già espresso nel parere sul futuro della privacy, secondo cui nel nuovo quadro legislativo globale dovrebbe essere inserito un principio generale di responsabilità. Lo scopo di tale disposizione

[4] www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

sarebbe quello di riaffermare e rafforzare l'"accountability" dei responsabili del trattamento dei dati personali. Ciò non pregiudica le misure di responsabilità concrete che potrebbero integrare questo principio.

26. Questa nuova disposizione sarebbe in linea con le disposizioni specifiche già esistenti nel quadro legislativo attuale. Si può citare in particolare l'articolo 6 della direttiva 95/46/CE, che al paragrafo 1 fa riferimento ai principi relativi alla qualità dei dati e al paragrafo 2 stabilisce che "[i]l responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1". la nuova disposizione sarebbe conforme anche all'articolo 17, paragrafo 1, in cui si stabilisce che il responsabile del trattamento deve attuare misure tecniche ed organizzative. In effetti, una norma generale sulla responsabilità rafforzerebbe la necessità che i responsabili del trattamento applichino le norme sulla sicurezza di cui all'articolo 17, in aggiunta a quanto previsto nelle rimanenti disposizioni.

III.2 Verso una proposta concreta per un principio generale di responsabilità

27. La nuova disposizione avrebbe lo scopo di promuovere l'adozione di misure concrete e pratiche, in quanto trasformerebbe i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del responsabile del trattamento, nel rispetto delle leggi e dei regolamenti applicabili. Il responsabile del trattamento dovrebbe anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni.

28. In modo schematico, una disposizione generale di questo tipo si incentrerebbe su due elementi principali:

    (i) la necessità che il responsabile del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati;
    (ii) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile del trattamento deve fornire la prova di quanto esposto al punto (i).

29. L'obbligo dovrebbe applicarsi a tutti i responsabili del trattamento e a tutte le situazioni.

30. Il primo elemento dell'obbligo imporrebbe ai responsabili del trattamento di attuare misure appropriate. I tipi di misure non sarebbero specificati nel testo della norma generale sulla responsabilità. Orientamenti successivi forniti dalle autorità nazionali di protezione dei dati, dal Gruppo di lavoro articolo 29 o dalla Commissione (attraverso procedure di comitatologia) potrebbero indicare, in determinati casi, un insieme minimo di misure specifiche costituenti misure appropriate. Un esempio di tali misure sarebbe l'adozione in alcuni casi di politiche e processi interni necessari per l'attuazione dei principi di protezione dei dati, che rispecchino le leggi e i regolamenti vigenti.

31. L'attuazione di tali misure e processi può anche avvenire in maniera efficace attraverso l'attribuzione di responsabilità e la formazione del personale impegnato nelle operazioni di trattamento. In particolare, conformemente all'articolo 18 della direttiva, i responsabili del trattamento devono essere incoraggiati a designare

incaricati della protezione dei dati personali. Si dovrebbe caldeggiare in ogni caso l'attribuzione di responsabilità a diversi livelli dell'organizzazione, in modo da renderle effettive.

32. Per quanto riguarda i trasferimenti di dati personali al di fuori dell'Unione europea, i responsabili del trattamento dovrebbero adottare ed attuare misure appropriate per ottemperare all'obbligo della presentazione di "garanzie sufficienti" di cui all'articolo 26 della direttiva, quali le regole d'impresa vincolanti.

33. I responsabili del trattamento dovrebbero altresì garantire che le misure pratiche attuate per conformarsi ai principi di protezione dei dati siano efficaci. Nel caso di trattamenti di dati di maggiori dimensioni, più complessi o ad alto rischio, l'efficacia delle misure adottate dovrebbe essere verificata periodicamente. Esistono diversi modi per valutare l'efficacia (o inefficacia) delle misure: monitoraggio, audit interni ed esterni, ecc.

34. In considerazione delle osservazioni svolte finora, il Gruppo di lavoro articolo 29 ha formulato una disposizione sostanziale che potrebbe essere introdotta in un quadro legislativo globale, il cui testo recita::

"Articolo X - Applicazione dei principi di protezione dei dati

1. Il responsabile del trattamento attua misure appropriate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati.
2 Su richiesta dell'autorità di vigilanza, il responsabile del trattamento dimostra la conformità con il paragrafo 1.

IV. ANALISI DI VARI ELEMENTI COLLEGATI AL PRINCIPIO GENERALE DI RESPONSABILITÀ

IV.1 Rafforzamento degli obblighi esistenti

35. Il Gruppo di lavoro articolo 29 rileva che alcuni responsabili del trattamento potrebbero percepire il principio generale di responsabilità come un'onerosa imposizione di nuovi obblighi giuridici in capo ai responsabili del trattamento, in particolare vista l'attuale difficile situazione economica dell'UE. Quest'interpretazione non sarebbe corretta.

36. Il Gruppo di lavoro articolo 29 desidera sottolineare che, per la maggior parte, gli obblighi contemplati nella nuova disposizione sono in realtà già previsti, anche se meno esplicitamente, dalla normativa vigente. Infatti, in forza dell'attuale quadro giuridico, i responsabili del trattamento sono tenuti a rispettare i principi e gli obblighi stabiliti dalla direttiva. A tal fine, è intrinsecamente necessario creare, ed eventualmente verificare, le procedure relative alla protezione dei dati. In quest'ottica, una disposizione sulla responsabilità non rappresenta una grande novità, e per la maggior parte non impone obblighi che non fossero già impliciti nella normativa vigente. In sintesi, la nuova disposizione non mira ad assoggettare

i responsabili del trattamento a nuovi principi, ma piuttosto a garantire di fatto l'effettiva osservanza di quelli esistenti.

37. In effetti, uno sviluppo legislativo in qualche modo simile è avvenuto nel 2009 in occasione della modifica della direttiva 2002/58[5], che ha imposto l'obbligo di attuare una politica di sicurezza, in particolare di "*garanti[re] l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali*". Così, per quanto riguarda le disposizioni di sicurezza di tale direttiva, il legislatore ha deciso che era necessario introdurre l'obbligo esplicito di predisporre e attuare una politica di sicurezza. Inoltre, l'articolo 18 della direttiva 95/46, che fa riferimento alla designazione di incaricati della protezione dei dati, accanto al sistema di regole d'impresa vincolanti di cui sopra, offrono già esempi di misure pratiche che possono essere adottate dai responsabili del trattamento.

38. Una questione collegata alla precedente riguarda le conseguenze connesse al rispetto (o al mancato rispetto) del principio di responsabilità. Il Gruppo di lavoro articolo 29 evidenzia che osservare il principio di responsabilità non significa necessariamente che il responsabile del trattamento agisca in conformità ai principi sostanziali enunciati nella direttiva, cioè esso non fornisce una presunzione legale di conformità né sostituisce tali principi. Il responsabile del trattamento può avere attuato e verificato le misure che ha posto in essere, e tuttavia può trovarsi coinvolto in irregolarità. Di conseguenza, l'adozione di misure volte al rispetto dei principi non deve in nessun caso esonerare i responsabili del trattamento dalle azioni di verifica dell'applicazione delle autorità di protezione dei dati. In pratica, i responsabili del trattamento del settore pubblico e privato che abbiano adottato misure nell'ambito di robusti programmi di conformità hanno maggiori probabilità di essere in regola con la legge. In effetti, poiché hanno predisposto misure efficaci dirette al rispetto dei principi sostanziali di protezione dei dati, dovrebbe essere meno probabile per loro incorrere in violazioni. Pertanto, nel valutare sanzioni relative a violazioni della privacy, le autorità di protezione dei dati potrebbero considerare rilevanti l'attuazione (o la mancata attuazione) delle misure e la loro verifica.

IV.2 Misure appropriate per l'attuazione delle disposizioni della direttiva

39. Una disposizione sulla responsabilità imporrebbe ai responsabili del trattamento di definire e attuare le misure necessarie per garantire il rispetto dei principi e degli obblighi della direttiva e di verificarne periodicamente l'efficacia.

40. Il principio generale di responsabilità proposto evita volutamente di precisare nei dettagli il tipo di misure da attuare. Ciò solleva le seguenti due questioni fondamentali interconnesse: *(i)* quali misure comuni soddisferebbero il principio di responsabilità? *(ii)* in che modo graduare e adattare le misure a circostanze specifiche?

---

[5] 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.

Le misure: descrizione

41. Il Gruppo di lavoro articolo 29 ritiene che le misure comuni concernenti la responsabilità potrebbero includere il seguente elenco non esaustivo:

    - istituzione di procedure interne *prima* della creazione di nuove operazioni di trattamento dei dati personali (revisione interna, valutazione, ecc.)[6];
    - formulazione per iscritto di politiche di protezione dei dati vincolanti da prendere in considerazione e applicare alle nuove operazioni di trattamento dei dati (ad esempio, qualità dei dati, comunicazione, principi di sicurezza, accesso, ecc.), che dovrebbero essere a disposizione degli interessati;
    - mappatura delle procedure per garantire la corretta identificazione di tutte le operazioni di trattamento dei dati e gestione di un inventario di dette operazioni;
    - nomina di un incaricato della protezione dei dati e di altri soggetti responsabili della protezione dei dati;
    - adeguata formazione e istruzione del personale in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (o responsabili) del trattamento dei dati personali (come i direttori delle risorse umane), ma anche dirigenti e sviluppatori in campo informatico, e direttori di unità commerciali. Dovrebbero essere stanziate risorse sufficienti per la gestione della privacy, ecc.;
    - creazione di procedure trasparenti per gli interessati finalizzate alla gestione delle richieste di accesso, rettifica e cancellazione;
    - istituzione di un meccanismo interno di gestione dei reclami;
    - definizione di procedure interne per la gestione e la comunicazione efficace di violazioni della sicurezza;
    - effettuazione di valutazioni d'impatto sulla privacy, in circostanze specifiche;
    - attuazione e controllo delle procedure di verifica per assicurare che tutte le misure esistano non solo sulla carta, ma siano applicate e funzionino nella pratica (audit interni o esterni ecc.).

42. Si potrebbe anche prevedere un approccio complementare al principio generale di responsabilità, secondo cui il quadro normativo includerebbe non solo un principio generale di responsabilità, ma anche un elenco illustrativo di misure che potrebbero essere incoraggiate a livello nazionale[7]. Questa disposizione potrebbe

---

6 Occorrerebbe un periodo di transizione per rendere le operazioni di trattamento dei dati in essere conformi alla normativa.

7 Per esempio, gli standard internazionali adottati a Madrid dalle autorità di protezione dei dati contengono all'articolo 22 una disposizione che prevede misure proattive, così formulata: "*Gli Stati devono incoraggiare, tramite la legislazione nazionale, l'attuazione, da parte di coloro che partecipano a qualsiasi fase del trattamento, di misure dirette a promuovere una migliore conformità alle leggi applicabili sulla protezione della privacy in relazione al trattamento dei dati personali. Tali misure potrebbero includere, tra l'altro:*

a) l'attuazione di procedure di prevenzione e di individuazione delle violazioni, che potrebbero basarsi sui modelli standardizzati di governance e/o di gestione della sicurezza dell'informazione;

b) la nomina di uno o più incaricati per la protezione dei dati o della privacy dotati di qualifiche, risorse e competenze adeguate a esercitare la loro funzione di sorveglianza in modo appropriato;

fornire un elenco esemplificativo e non esaustivo di misure che potrebbero costituire uno "strumentario" per i responsabili del trattamento, offrendo loro orientamenti su quali potrebbero essere, a seconda dei casi, le misure appropriate da adottare. Tale elenco esemplificativo sarebbe ovviamente soltanto un complemento all'obbligo giuridico generale di adottare le misure appropriate.

Graduare le misure

43. Quello che precede costituisce un elenco esemplificativo di misure che i responsabili del trattamento potrebbero realizzare per ottemperare alla prima parte del principio di responsabilità (*Il responsabile del trattamento attua misure appropriate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati).*

44. Alcune delle misure sono "elementi base" che dovranno essere attuati nella maggior parte delle operazioni di trattamento. L'elaborazione di politiche e procedure interne di attuazione dei principi (procedure per gestire le richieste di accesso e i reclami) potrebbe costituire un esempio di misure appropriate per alcuni trattamenti di dati. L'idoneità delle misure dovrà essere decisa caso per caso. Spetta ai responsabili del trattamento prendere tali decisioni, seguendo gli orientamenti emessi dalle autorità nazionali di protezione dei dati e dal Gruppo di lavoro articolo 29, se disponibili (v. sotto).

45. Da quanto precede risulta che nel determinare i tipi di azioni da attuare, non esistono alternative valide alle soluzioni "su misura". Infatti, le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati. Un approccio uguale per tutti avrebbe il solo effetto di costringere i responsabili del trattamento all'interno di strutture inadatte e si rivelerebbe quindi fallimentare.

46. Secondo questo approccio, i responsabili del trattamento devono essere in grado di adattare le misure alle specificità concrete delle loro situazioni particolari e delle operazioni di trattamento dei dati in questione. In questo contesto, il Gruppo di

---

c) la regolare attuazione di programmi di formazione, istruzione e sensibilizzazione rivolti ai membri delle organizzazioni per una migliore comprensione delle leggi applicabili in materia di tutela della privacy in relazione al trattamento dei dati personali, nonché procedure stabilite a tal fine dalle organizzazioni;

d) l'effettuazione periodica di audit trasparenti, realizzati da soggetti qualificati e preferibilmente indipendenti per verificare la conformità con le leggi vigenti in materia di protezione della privacy in relazione al trattamento dei dati personali, e con le procedure stabilite a tal fine dalle organizzazioni;

e) l'adeguamento delle tecnologie e/o dei sistemi informatici per il trattamento dei dati personali alle leggi vigenti sulla tutela della privacy in relazione al trattamento dei dati personali, in particolare al momento di decidere le specifiche tecniche, lo sviluppo e l'attuazione;

f) la realizzazione di valutazioni d'impatto sulla privacy prima dell'attuazione di nuove tecnologie e/o nuovi sistemi informatici per il trattamento dei dati personali, e prima dell'applicazione di nuovi metodi di trattamento dei dati personali o di qualunque modifica sostanziale nel trattamento esistente;

g) l'adozione di codici di autoregolamentazione vincolanti, che includano elementi per misurarne l'efficacia in termini di conformità e di livello di protezione dei dati personali, e che prevedano misure efficaci in caso di non conformità;

h) l'attuazione di un piano d'azione che stabilisca orientamenti per l'azione da intraprendere in caso di violazione delle leggi sulla tutela della privacy in relazione al trattamento dei dati personali, compreso quanto meno l'obbligo di determinare la causa e l'entità della violazione, di descriverne gli effetti negativi e di adottare le misure appropriate per evitare che si ripeta in futuro."

lavoro articolo 29 rammenta i criteri di cui all'articolo 17 dell'attuale direttiva[8] per determinare il tipo di misure di sicurezza da applicare, ossia i rischi rappresentati dal trattamento dei dati e dalla loro natura. Questi due fattori potrebbero essere utilizzati per analogia per determinare i tipi generali di misure da applicare. Più concretamente, taluni aspetti come le dimensioni delle operazioni di trattamento, gli obiettivi dello stesso e il numero di trasferimenti di dati previsti possono contribuire a definire il livello di rischio. Occorre altresì tenere conto del tipo di dati, in particolare se si tratta o meno di dati sensibili. Si potrebbe inoltre riflettere sulla necessità di imporre determinati obblighi all'incaricato del trattamento o ai progettisti e/o produttori di tecnologie dell'informazione e della comunicazione alla luce di questo principio di responsabilità.

47. In base a tali criteri, in linea di principio, i grandi responsabili del trattamento dovrebbero attuare misure rigorose. In alcuni casi, può essere necessario anche per i piccoli e medi responsabili del trattamento presentare garanzie rigorose, per esempio se sono impegnati in operazioni rischiose di trattamento dei dati, come alcune operazioni nel quadro dei servizi sanitari online. Ad esempio, un ente locale (municipio), una multinazionale, una piccola impresa (Internet), un'organizzazione la cui attività principale sia il trattamento dei dati o un organizzazione che abbia commesso violazioni in passato richiederebbero tutti misure specifiche, al fine di garantire una governance credibile ed efficace delle informazioni. Come risultato, nei casi più semplici e basilari, come per il trattamento dei dati personali relativi a risorse umane per la creazione di una directory, l'"obbligo di dimostrare", cui si fa riferimento nel paragrafo 2 della disposizione sulla responsabilità, potrebbe essere rispettato facilmente (attraverso, ad esempio, le note informative utilizzate, la descrizione delle misure di sicurezza di base, ecc.). Al contrario, in altri casi più complessi, come ad esempio l'utilizzo di dispositivi biometrici innovativi, l'adempimento dell'"obbligo di dimostrare" potrebbe richiedere altre misure. Il responsabile del trattamento potrebbe ad esempio dover dimostrare di aver effettuato una valutazione d'impatto sulla privacy, che il personale che si occupa del trattamento ha ricevuto formazioni e informazioni su base regolare, ecc.

48. La trasparenza è parte integrante di molte misure concernenti responsabilità. La trasparenza nei confronti degli interessati e del pubblico in generale contribuisce alla responsabilità dei responsabili del trattamento. Per esempio, un maggiore livello di responsabilità si consegue pubblicando su Internet le politiche in materia di privacy, fornendo trasparenza riguardo alle procedure interne di gestione dei reclami, e attraverso la pubblicazione di relazioni annuali.

Orientamento e certezza del diritto

49. Mentre l'esigenza di adattabilità e quindi di una certa flessibilità richiede l'uso di un linguaggio aperto, il Gruppo di lavoro articolo 29 è consapevole del fatto che una disposizione di massima che lasci spazio a flessibilità e adattabilità potrebbe anche causare incertezza. I responsabili del trattamento potrebbero ritenere che la

---

8 "*Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere".*

disposizione non sia sufficientemente precisa per garantire la certezza del diritto. Per esempio, potrebbero nutrire dubbi circa il livello di dettaglio richiesto per le politiche e le procedure sulla privacy, per i tempi e i modi per designare l'incaricato della protezione dei dati, per l'organizzazione di sessioni di formazione, ecc. L'incertezza potrebbe riguardare anche il tipo di verifica necessario, da parte di terzi ovvero interno. Inoltre, i responsabili del trattamento potrebbero anche temere di essere oggetto di interpretazioni divergenti e arbitrarie a livello nazionale per quanto riguarda la portata e la natura dei loro obblighi.

50. Il Gruppo di lavoro articolo 29 comprende questa preoccupazione. Tuttavia, per le ragioni esposte in precedenza circa l'esigenza di flessibilità e di adattabilità, la soluzione per conseguire la certezza del diritto non può essere fornita nella direttiva stessa. A tal fine, il Gruppo di lavoro articolo 29 ritiene che gli orientamenti per l'armonizzazione emanati dalla Commissione (per esempio, tramite misure tecniche di attuazione) e/o dallo stesso Gruppo di lavoro possano diventare uno strumento utile per fornire maggiore certezza ed eliminare potenziali differenze a livello di attuazione[9]. Il Gruppo di lavoro potrebbe anche preparare orientamenti generali che forniscano una base di elementi necessari per un responsabile del trattamento standard. Questa base potrebbe essere adattata alle esigenze specifiche di ciascun responsabile del trattamento di dati.

51. Potrebbe anche essere utile sviluppare un *programma modello per la conformità dei dati*, che potrebbe essere utilizzato da responsabili del trattamento di medie e grandi dimensioni come base su cui elaborare i loro programmi particolari, come è avvenuto per le regole d'impresa vincolanti elaborate sulla base degli orientamenti del Gruppo di lavoro articolo 29[10]. Tali modelli dovrebbero essere creati in seguito a un attento riesame delle prassi correnti e dei modelli disponibili, e previa consultazione di tutte le parti interessate. Si tratta di un settore che richiederà investimenti ingenti da parte di tutti i soggetti coinvolti.

Efficacia delle misure

52. Le stesse questioni trattate in precedenza riguardanti le misure applicabili emergono nel contesto della necessità di garantirne l'efficacia. Il modo in cui questa può essere assicurata sarà diverso a seconda del tipo di trattamento dei dati.

53. Esistono vari metodi a disposizione dei responsabili del trattamento per valutare l'efficacia (o l'inefficacia) delle misure. Per il trattamento di dati di maggiori dimensioni, più complesso e ad alto rischio, gli audit interni ed esterni sono metodi comuni di verifica. Anche il modo in cui vengono condotti gli audit può variare, da audit completi ad audit negativi (che possono a loro volta assumere forme diverse). Nel decidere come garantire l'efficacia delle misure, il Gruppo di lavoro articolo 29 suggerisce di utilizzare gli stessi criteri applicati per decidere le

---

9 Un esempio di questo tipo di orientamento è lo strumento di autovalutazione PIPEDA, pubblicato dall'Ufficio del commissario canadese per la privacy per aiutare i responsabili del trattamento di medie e grandi dimensioni a sviluppare ed attuare una buona governance e gestione della privacy. Lo strumento di autovalutazione è disponibile all'indirizzo: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf .

10 Documento di lavoro 153 del Gruppo di lavoro articolo 29 che stabilisce una tabella comprendente gli elementi e i principi delle regole d'impresa vincolanti e documento di lavoro 154 che stabilisce un quadro per la struttura delle regole d'impresa vincolanti.

misure mutuati dall'articolo 17 della direttiva 95/46/CE, vale a dire, i rischi presentati dal trattamento e la natura dei dati. Pertanto, il modo in cui un responsabile del trattamento deve assicurare l'efficacia delle misure dipende dalla sensibilità dei dati, dalla quantità dei dati trattati e dai particolari rischi che il trattamento comporta . Gli orientamenti del Gruppo di lavoro relativi alle misure potrebbero comprendere anche indicazioni su questo aspetto.

IV.3 Collegamento con altri obblighi

Notificazioni preliminari

54. Si potrebbe intraprendere una riflessione sul possibile impatto sulle notificazioni preliminari quando adeguate garanzie siano definite a livello del responsabile del trattamento. Si potrebbe prevedere la possibilità che determinati meccanismi di responsabilità sostituiscano o riducano gli obblighi amministrativi dell'attuale legislazione sulla protezione dei dati, come già suggerito dal Gruppo di lavoro articolo 29 nel suo parere sul futuro della privacy.

Trasferimenti internazionali di dati

55. Le regole d'impresa vincolanti rappresentano un esempio di attuazione dei principi di protezione dei dati sulla base del principio di responsabilità. Si tratta di una modalità individuata e accettata dal Gruppo di lavoro articolo 29 per fornire adeguate garanzie per i trasferimenti al di fuori dell'Unione europea.

56. Questo è un settore che trarrebbe beneficio da un'ulteriore analisi alla luce della revisione della direttiva 95/46. In particolare, sarebbe importante esaminare se nell'ambito di applicazione dell'articolo 26, paragrafo 2, della direttiva (*uno Stato membro può autorizzare un trasferimento [...] qualora il responsabile del trattamento presenti garanzie sufficienti […]; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate")* rientrino a pieno titolo le regole d'impresa vincolanti e altri meccanismi analoghi di responsabilità vincolanti quali strumenti atti a fornire garanzie sufficienti.

57. In questo contesto, è molto importante valutare, tra l'altro, i meccanismi usati per dare attuazione ai principi e agli obblighi di protezione dei dati all'interno degli stessi responsabili del trattamento e dei sistemi di verifica. È inoltre importante analizzare i meccanismi per ottimizzare l'attuale sistema basato sull'autorizzazione dei trasferimenti di dati da parte delle autorità nazionali di protezione dei dati.

IV.4 Il ruolo delle autorità di protezione dei dati

58. Una questione da affrontare è se il principio di responsabilità proposto nel presente parere influirà sui poteri delle autorità di protezione dati, in particolare in sede di verifica dell'applicazione. Come ulteriormente descritto di seguito, il principio non sottrae alcun potere alle autorità di protezione dei dati, bensì apporterà loro vantaggi.

59. Per quanto riguarda la verifica dell'applicazione, il principio proposto riconosce la competenza delle autorità di protezione dei dati a chiedere al titolare del trattamento la prova della conformità con il principio di responsabilità, rafforzandone così i poteri. Questo garantisce che le autorità mantengano, in qualsiasi momento, la competenza a svolgere azioni di verifica. . Occorre chiarire che, in ogni caso, le autorità di protezione dei dati resterebbero competenti a controllare non solo le misure adottate dai responsabili del trattamento, ma anche e soprattutto il rispetto dei principi e degli obblighi di fondo.

60. Inoltre, l'attuazione del principio di responsabilità fornirà alle autorità di protezione dei dati informazioni utili per monitorare i livelli di conformità. Infatti, poiché i responsabili del trattamento dovranno essere in grado di dimostrare alle autorità se e come hanno attuato le misure, le autorità in discorso disporranno di informazioni altamente rilevanti in materia di conformità e potranno in seguito utilizzare tali informazioni nel contesto delle loro azioni di verifica dell'applicazione. Inoltre, se tali informazioni non sono fornite su richiesta, le autorità di protezione dei dati avranno un motivo per agire immediatamente contro i responsabili del trattamento, indipendentemente dalla presunta violazione di altri principi basilari di protezione dei dati.

61. Il principio dovrebbe anche essere utile alle autorità di protezione dei dati in quanto le aiuterebbe ad essere più selettive e strategiche, consentendo loro di investire le proprie risorse in modo da generare il maggior livello possibile di conformità.

62. Il Gruppo di lavoro articolo 29 osserva che il principio di responsabilità potrebbe contribuire allo sviluppo di competenze giuridiche e tecniche nel campo dell'attuazione delle disposizioni sulla protezione dei dati. Saranno indispensabili in questo settore persone altamente competenti, dotate di approfondite conoscenze tecniche e giuridiche in materia di protezione dei dati, nonché di capacità di comunicare, formare il personale, elaborare e attuare politiche e svolgere audit. Tali competenze saranno necessarie sia internamente sia nella forma di servizi esterni che le imprese potranno richiedere. Questa evoluzione sarà fondamentale per garantire che i responsabili del trattamento possano svolgere i propri compiti, compreso, se necessario, lo svolgimento di audit interni ed esterni/interni. Al tempo stesso, questo sviluppo sarà positivo per le autorità di protezione dei dati, poiché il sistema contribuirà alla conformità in generale, le autorità avranno a loro disposizione informazioni più affidabili riguardo alle pratiche interne delle società, e la formazione di professionisti qualificati con conoscenze approfondite in materia di protezione dei dati sarà certamente di aiuto nella loro interazione con i responsabili del trattamento.

63. Si può concludere che il ruolo delle autorità di protezione dei dati si traduce prevalentemente in attività "ex post" piuttosto che "ex ante". Poiché la responsabilità pone l'accento su determinati risultati da raggiungere in termini di buona governance della protezione dei dati, si dice che è orientata ai risultati ed incentrata sull'aspetto "ex post" (cioè, successivo all'inizio del trattamento dei dati).

IV. 5 Sanzioni

64. Il sistema proposto può funzionare solo se le autorità di protezione dei dati sono dotate di poteri sanzionatori di una certa entità. In particolare, quando e se i responsabili del trattamento non riescono a soddisfare il principio di responsabilità, sorge la necessità di sanzioni appropriate. Per esempio, deve essere punibile il mancato rispetto da parte di un responsabile del trattamento degli impegni formulati nel quadro di politiche interne vincolanti. Ovviamente, ciò si aggiunge all'effettiva violazione dei principi sostanziali di protezione dei dati.

65. Inoltre, il Gruppo di lavoro articolo 29 ritiene che i poteri delle autorità nazionali di protezione dei dati debbano comprendere la possibilità di imporre ai responsabili del trattamento istruzioni precise riguardo al loro sistema di conformità.

IV.6 Lo sviluppo di sistemi di certificazione

66. Nel lungo periodo, la disposizione sulla responsabilità potrebbe favorire lo sviluppo di programmi o sigilli di certificazione. Tali programmi contribuirebbero a dimostrare che un responsabile del trattamento ha rispettato la disposizione e che, quindi, ha definito e attuato misure appropriate che sono state periodicamente sottoposte a revisione. Vari fattori, illustrati di seguito, potrebbero favorire tale sviluppo.

67. In generale, si può prevedere che, per differenziarsi, i servizi di protezione dei dati/auditing/valutazione d'impatto sulla privacy offriranno probabilmente sempre più spesso certificati o sigilli per distinguersi all'interno del mercato e anche per acquisire un vantaggio competitivo. I responsabili del trattamento potrebbero decidere di avvalersi di servizi affidabili che rilasciano certificati. Mano a mano che acquisteranno notorietà in virtù delle verifiche rigorose, i sigilli di certificazione potranno riscuotere il favore dei responsabili del trattamento in quanto più "comodi" in termini di sicurezza oltre che più vantaggiosi sul piano competitivo.

68. L'uso di regole d'impresa vincolanti come base giuridica per i trasferimenti internazionali di dati implica che i responsabili del trattamento dimostrino di aver messo in atto adeguate garanzie, nel cui caso le autorità di protezione dei dati possono autorizzare i trasferimenti. Questo è un ambito in cui i servizi di certificazione potrebbero essere utili. Tali servizi analizzerebbero le assicurazioni fornite dal responsabile del trattamento e, se del caso, emetterebbero il relativo sigillo di certificazione. Un'autorità di protezione dei dati potrebbe utilizzare la certificazione fornita da un dato programma di certificazione nella sua analisi delle regole d'impresa vincolanti tesa a verificare se un responsabile del trattamento abbia fornito garanzie sufficienti ai fini dei trasferimenti internazionali di dati, contribuendo così all'ottimizzazione del processo di autorizzazione di tali trasferimenti.

IV.7 La regolamentazione dei sistemi di certificazione

69. Le stesse ragioni che favoriscono lo sviluppo di servizi di certificazione avvalorano la necessità che tali servizi siano regolamentati. Infatti, se tali servizi sono intesi a fornire prove affidabili di conformità in termini di protezione dei dati (alle autorità di protezione dei dati, ai responsabili del trattamento e ai consumatori in generale) e a funzionare correttamente nel mercato interno, risultano necessarie norme disciplinanti la fornitura di tali servizi. Le autorità di protezione dei dati dovrebbero svolgere un ruolo chiave nello sviluppo di tali norme (ad esempio modelli, ecc.) e dovrebbero essere in grado di farne rispettare l'attuazione. Ciò impone altresì che siano dotate di risorse sufficienti. Inoltre, le autorità di protezione dei dati dovrebbero svolgere un ruolo nella certificazione dei certificatori. Questo potrebbe essere particolarmente importante nell'ambito dei trasferimenti internazionali di dati. Poiché la qualità dei servizi e il loro funzionamento nel mercato interno sono un criterio fondamentale, la legge dovrà stabilire le condizioni atte a conseguire tale qualità. Non sembra un'opzione possibile lasciare questo aspetto al mercato. L'esperienza in altri settori, ad esempio la certificazione delle merci, ha mostrato una tendenza al ribasso. La concorrenza tra i prestatori di servizi può condurre ad una riduzione dei prezzi e anche a una certa flessibilità o rilassamento delle procedure. In sintesi, in ambito transfrontaliero o meno, le risultano necessarie norme dirette a garantire la buona qualità dei servizi e una base di parità.

70. Il Gruppo di lavoro articolo 29 osserva che la legislazione vigente in materia di accreditamento[11] potrebbe essere applicabile nel settore dei servizi di certificazione nel campo della protezione dei dati. Tale normativa fornisce già la struttura necessaria, stabilendo norme sull'organizzazione e il funzionamento degli organismi di accreditamento. Queste regole valgono per l'accreditamento facoltativo e anche nei casi specifici in cui l'accreditamento è obbligatorio.

71. Ovviamente, questo tipo di servizio darebbe altresì un impulso all'armonizzazione delle norme di base rispetto alle quali i soggetti sarebbero sottoposti a verifica. Gli orientamenti menzionati (elaborati dal gruppo articolo 29 o dalla Commissione), indicando programmi modello di conformità dei dati, sarebbero di grande utilità.

V. CONCLUSIONI

72. Lo sviluppo di nuove tecnologie e la costante globalizzazione dell'economia e della società hanno condotto ad una proliferazione di dati personali raccolti, selezionati, trasferiti o altrimenti conservati. I rischi connessi a tali dati, pertanto, si moltiplicano.

73. Il Gruppo di lavoro articolo 29 è convinto che l'aumento sia dei rischi sia del valore dei dati personali in sé renda necessario rafforzare il ruolo e la responsabilità dei responsabili del trattamento. Un quadro normativo che provveda a questa nuova realtà deve contenere gli strumenti necessari per incoraggiare i

[11] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93.

responsabili del trattamento ad applicare in pratica misure appropriate ed efficaci in grado di realizzare i risultati derivanti dai principi di protezione dei dati. Esempi di tali misure sono le procedure per garantire l'identificazione di tutte le operazioni di trattamento dei dati e per rispondere alle richieste di accesso, lo stanziamento di risorse e la designazione di persone responsabili per l'organizzazione della conformità della protezione dei dati.

74. Per incoraggiare la protezione dei dati nella pratica, il Gruppo di lavoro articolo 29 propone in primo luogo di includere nelle proposte di modifica della direttiva sulla protezione dei dati una nuova disposizione che obblighi i responsabili del trattamento ad attuare misure appropriate ed efficaci per garantire che i principi e gli obblighi della direttiva sulla protezione dei dati siano rispettati e di dimostrarlo, su richiesta, alle autorità. Tali misure dovrebbero favorire il rispetto dei principi e degli obblighi di protezione dei dati, riducendo al minimo i rischi di accesso non autorizzato, uso improprio, perdita, ecc. L'obbligo di dimostrare, su richiesta, la predisposizione delle misure necessarie dovrebbe diventare uno strumento utile alle autorità di protezione dei dati nello svolgimento dei loro compiti di verifica dell'applicazione.

75. L'obbligo di attuare tali misure dovrebbe applicarsi ai responsabili del trattamento di tutti i settori (pubblico e privato) ed essere adattabile, di modo che il tipo di misure sia adeguato ai rischi presentati dal trattamento e alla natura dei dati.

Fatto a Bruxelles, 13 luglio 2010

Per il Gruppo di lavoro,
Il presidente
Jacob KOHNSTAMM