

Gruppo di lavoro articolo 29 per la protezione dei dati - Parere 16/02/2010, n. WP169

Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento".
Emanato dal Gruppo di lavoro articolo 29 per la protezione dei dati.

Sintesi

Il concetto di "responsabile del trattamento" dei dati, e la sua interazione col concetto di "incaricato del trattamento", svolgono un ruolo cruciale nell'applicazione della direttiva 95/46/CE, poiché determinano chi risponde dell'osservanza delle norme relative alla protezione dei dati, il modo in cui gli interessati possono esercitare i loro diritti, il diritto nazionale applicabile e l'efficacia del lavoro delle autorità per la protezione dei dati.

La differenziazione organizzativa nel settore pubblico e privato, lo sviluppo delle TIC e la dimensione mondiale del trattamento dei dati aumentano la complessità di tale trattamento e rendono necessario un chiarimento dei concetti sopra indicati, per garantirne un'efficace applicazione e osservanza nella pratica.

Il concetto di responsabile del trattamento è autonomo - va interpretato cioè principalmente alla luce delle disposizioni comunitarie relative alla protezione dei dati -, e funzionale, nel senso che è finalizzato all'assegnazione di responsabilità laddove intervenga un'influenza effettiva: si basa quindi su un'analisi fattuale piuttosto che formale.

La definizione della direttiva si articola intorno a tre componenti principali:

- il soggetto ("la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo");
- la possibilità di una responsabilità plurima ("che, da solo o insieme ad altri"), e
- gli aspetti principali che distinguono il responsabile del trattamento da altre figure ("determina le finalità e gli strumenti del trattamento di dati personali").

L'analisi di queste componenti porta a una serie di conclusioni sintetizzate nella parte IV del presente parere.

Nel presente documento viene poi analizzato il concetto di incaricato del trattamento, la cui esistenza dipende da una decisione presa dal responsabile del trattamento. Quest'ultimo può decidere o di trattare i dati all'interno della propria organizzazione o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna. Per poter agire come incaricato del trattamento occorrono due requisiti: essere una persona giuridica distinta dal responsabile del trattamento ed elaborare i dati personali per conto di quest'ultimo.

Il Gruppo di lavoro riconosce le difficoltà che presenta l'applicazione delle definizioni della direttiva in un contesto complesso, con vari scenari che possono vedere intervenire responsabili e incaricati del trattamento, da soli o congiuntamente con altri, con vari gradi d'autonomia e di responsabilità.

Nella sua analisi, il Gruppo di lavoro sottolinea la necessità di attribuire le responsabilità in modo tale da garantire nella pratica un'adeguata osservanza delle norme sulla protezione dei dati. Ritiene comunque che non vi sia alcun motivo di pensare che, in tale ottica, l'attuale distinzione fra responsabili del trattamento e incaricati del trattamento possa perdere rilevanza e praticabilità.

Il Gruppo di lavoro spera pertanto che le spiegazioni date nel presente parere, corredate di specifici esempi tratti dall'esperienza quotidiana delle autorità per la protezione dei dati personali, contribuiranno a fornire effettivi orientamenti sul modo in cui interpretare queste definizioni chiave della direttiva.

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 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, della succitata 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:

I. Introduzione

Il concetto di "responsabile del trattamento" e la sua interazione con quello di "incaricato del trattamento" svolgono un ruolo fondamentale nell'applicazione della [direttiva 95/46/CE](#), poiché determinano chi risponde dell'osservanza delle norme relative alla protezione dei dati e il modo in cui gli interessati possono esercitare in pratica i loro diritti. Il concetto di "responsabile del trattamento" è fondamentale anche per stabilire il diritto nazionale applicabile e per l'efficace esercizio dei compiti di controllo conferiti alle autorità per la protezione dei dati.

È quindi importantissimo che il preciso significato di questi concetti e che i criteri per il loro corretto utilizzo siano sufficientemente chiari e condivisi da tutti coloro che, negli Stati membri, si occupano dell'attuazione della direttiva e dell'applicazione, valutazione ed esecuzione delle disposizioni nazionali che la recepiscono.

Sembrerebbe che vi sia una mancanza di chiarezza, perlomeno quanto a certi aspetti di tali nozioni, ed alcuni punti di vista divergenti fra gli interlocutori nei vari Stati membri, cosa che potrebbe portare a interpretazioni diverse degli stessi principi e definizioni introdotti a fini di armonizzazione a livello europeo. Il Gruppo di lavoro Articolo 29 ha quindi deciso, nell'ambito del suo programma di lavoro strategico 2008-2009, di dedicare speciale attenzione alla stesura di un documento contenente un approccio comune a tali questioni.

Il Gruppo di lavoro riconosce che l'applicazione concreta dei concetti di "responsabile del trattamento" e "incaricato del trattamento" sta diventando sempre più complicata. Ciò è dovuto per lo più alla crescente complessità dei contesti in cui sono utilizzati, ed in particolare ad una sempre più spiccata tendenza, sia nel settore privato che in quello pubblico, alla differenziazione organizzativa, associata allo sviluppo delle TIC e alla globalizzazione: tali fattori possono far sorgere nuove e difficili problematiche e a volte incidere negativamente sul livello di protezione degli interessati.

Benché le disposizioni della direttiva siano state formulate in un modo neutro sotto il profilo tecnologico e finora abbiano potuto resistere bene ad un contesto in costante evoluzione, queste complessità possono effettivamente generare incertezze per quanto riguarda l'attribuzione delle responsabilità e il campo d'applicazione delle legislazioni nazionali rilevanti. Tali incertezze possono a loro volta inficiare il rispetto delle norme relative alla protezione dei dati in settori critici e l'efficacia della normativa sulla protezione dei dati nel suo insieme. Il Gruppo di lavoro ha già affrontato alcune di queste problematiche in relazione a specifiche questioni [1], ma ritiene che ora sia necessario formulare orientamenti più elaborati e una guida più specifica per garantire un approccio coerente e armonizzato.

Il Gruppo di lavoro ha quindi deciso di fornire nel presente parere - analogamente a quanto già fatto per il concetto di dati personali [2] - alcuni chiarimenti ed esempi concreti [3] relativamente alle nozioni di "responsabile del trattamento" e "incaricato del trattamento".

[1] Cfr. ad es. il parere 10/2006 sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT), adottato il 22 novembre 2006 (WP 128), e più recentemente il parere 5/2009 sui social network on-line, adottato il 12 giugno 2009 (WP 163).

[2] Parere 4/2007 sul concetto di dati personali, adottato il 20 giugno 2007 (WP 136).

[3] Si tratta di esempi basati su attuali prassi nazionali od europee, eventualmente modificati o adattati ai fini di una migliore comprensione.

II. Osservazioni generali e questioni politiche

La direttiva si riferisce esplicitamente al concetto di "responsabile del trattamento" in diverse disposizioni. Le definizioni di "responsabile del trattamento" e di "incaricato del trattamento", di cui all'articolo 2, lettere d) ed e) della [direttiva 95/46/CE](#) (in appresso "la direttiva") sono le seguenti:

"responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;

"incaricato del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento.

Queste definizioni hanno preso forma durante i negoziati sul progetto di proposta della direttiva nei primi anni '90: il concetto di "responsabile del trattamento" (controller) è stato essenzialmente mutuato dalla Convenzione 108 del Consiglio d'Europa, stipulata nel 1981. Nel corso dei negoziati sono intervenuti alcuni grossi cambiamenti.

In primo luogo, il termine della Convenzione 108 "responsabile del casellario" (controller of the file) è stato sostituito da "responsabile del trattamento" in relazione al "trattamento di dati personali". Quest'ultima è una nozione ampia, definita all'articolo 2, lettera b) della direttiva come "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 conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione." Il concetto di responsabile, controller, non è stato quindi più riferito a un oggetto statico ("il casellario"), bensì ricollegato ad attività rispecchianti il ciclo di vita delle informazioni, dalla raccolta alla distruzione - aspetti da esaminarsi in dettaglio e nell'insieme ('operazione o insieme di operazioni'). Anche se il risultato poteva risultare identico in molti casi, la nozione in oggetto ha in questo modo acquisito un significato e una portata molto più ampi e dinamici.

Altri cambiamenti riguardano; l'introduzione della possibilità di una "responsabilità plurima" ("da solo o insieme ad altri"); la funzione attribuita al responsabile del trattamento, che è quella di determinare "le finalità e gli strumenti del trattamento di dati personali", e il fatto che questa determinazione possa essere fissata da disposizioni legislative nazionali o comunitarie o in altro modo. La direttiva introduce inoltre la nozione di "incaricato del trattamento", che non figura nella Convenzione 108. Questi ed altri cambiamenti saranno analizzati più dettagliatamente nel seguito del presente parere.

II.1. Ruolo dei concetti

Mentre il concetto di responsabile (del casellario) ha un ruolo estremamente limitato [4] nella Convenzione 108, così non è nella direttiva, il cui articolo 6, paragrafo 2 stabilisce esplicitamente che "il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1" - ossia dei principi fondamentali relativi alla qualità dei dati, fra cui quello, sancito all'articolo 6, paragrafo 1, lettera a), secondo cui "i dati personali devono essere trattati lealmente e lecitamente". Ciò significa di fatto che tutte le disposizioni relative alle condizioni per il trattamento lecito dei dati si rivolgono al responsabile del trattamento, anche se non è sempre chiaramente indicato.

Anche le disposizioni sui diritti dell'interessato (informazione, accesso, rettifica, cancellazione, congelamento e opposizione al trattamento dei dati personali (articoli 10-12 e 14)) sono state formulate in modo tale da creare obblighi per il responsabile del trattamento, la cui figura è inoltre centrale nelle disposizioni sulla notificazione e il controllo preliminare (articoli 18-21). Non sorprende, infine, il fatto che il responsabile del trattamento debba anche rispondere, in linea di principio, per eventuali danni cagionati da un trattamento illecito (articolo 23).

Ciò significa che il concetto di responsabile del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati, e il modo in cui gli interessati possono esercitare in pratica i loro diritti [5] - serve, in altre parole, ad attribuire responsabilità.

Questo ci riporta all'aspetto centrale della direttiva, il cui principale obiettivo è "la tutela delle persone fisiche con riguardo al trattamento dei dati personali". Tale obiettivo può essere raggiunto e messo in pratica solo se i responsabili del trattamento dei dati vengono adeguatamente spinti, da mezzi giuridici e di altro tipo, ad adottare tutte le misure necessarie per garantire un'effettiva protezione. Ciò trova conferma all'articolo 17, paragrafo 1 della direttiva, che stabilisce che il responsabile del trattamento "deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali"

I mezzi per incentivare la responsabilità possono essere proattivi e reattivi. Nel primo caso servono a garantire un'efficace applicazione delle misure di protezione dei dati e mezzi sufficienti per permettere ai responsabili del trattamento di rendere conto delle loro attività. Nel secondo caso possono chiamare in causa la responsabilità civile e sanzioni per garantire il risarcimento di eventuali danni di una certa entità e l'adozione di misure adeguate per riparare possibili errori o irregolarità.

Il concetto di responsabile del trattamento è inoltre un elemento fondamentale per determinare il diritto nazionale applicabile a un trattamento o a un insieme di trattamenti. La principale disposizione relativa al diritto applicabile, di cui all'articolo 4, paragrafo 1 della direttiva, prevede che ciascuno Stato membro applichi le proprie disposizioni nazionali "al trattamento di dati personali [...] effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro". E la disposizione continua nel modo seguente: "qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile". Ciò significa che lo o gli stabilimenti del responsabile del trattamento determinano anche il o i diritti nazionali applicabili, ed eventualmente una serie di leggi nazionali applicabili e il modo in cui sono collegate fra di loro. [6]

Va infine osservato che il concetto di "responsabile del trattamento" appare in molte disposizioni della direttiva come un elemento del loro campo d'applicazione o come specifica condizione applicabile. L'articolo 7, ad esempio, stabilisce che il trattamento di dati personali può essere effettuato soltanto quando: "c) è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento [...], e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, oppure f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano...". L'identità del responsabile del trattamento è inoltre un importante elemento delle informazioni da fornire all'interessato ai sensi degli articoli 10 e 11.

Il concetto di "incaricato del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti (articoli 16-17), poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del responsabile del trattamento o per suo conto. La distinzione fra i due concetti serve per lo più a differenziare fra la persona che ha l'effettiva responsabilità in qualità di "responsabile del trattamento", e la persona che agisce semplicemente per conto di quest'ultimo. È, ancora una volta, soprattutto una questione di attribuzione di responsabilità, da cui possono poi derivare altre conseguenze, per quanto riguarda il diritto applicabile o altri aspetti.

Nel caso dell'incaricato del trattamento vi è comunque un'ulteriore conseguenza - che interessa anche

il responsabile del trattamento: ai sensi dell'articolo 17 della direttiva, il diritto applicabile alla sicurezza dei trattamenti è quello dello Stato membro nel quale è stabilito l'incarico del trattamento. [7]

Infine, secondo la definizione dell'articolo 2, lettera f), "si intende per [...] 'terzi': la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia la persona interessata, il responsabile del trattamento, l'incarico del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta." Il responsabile del trattamento, l'incarico del trattamento e il loro staff sono quindi considerati il "nucleo centrale" del trattamento dei dati, e non rientrano nel campo d'applicazione delle particolari disposizioni relative ai terzi.

II.2. Contesto rilevante

I vari sviluppi che hanno caratterizzato il contesto interessato hanno reso le questioni in oggetto più urgenti ed anche più complesse. All'epoca della firma della Convenzione 108 e, in larga misura, anche al momento dell'adozione della [direttiva 95/46/CE](#), l'ambito del trattamento dei dati era ancora relativamente chiaro e semplice. La situazione oggi è diversa.

Ciò è dovuto, in primo luogo, a una crescente tendenza alla differenziazione organizzativa nella maggior parte dei settori interessati. Nel settore privato, la ripartizione dei rischi, finanziari o d'altro tipo, ha portato ad una continua diversificazione delle imprese, ancora più accentuata da fusioni e acquisizioni. Nel settore pubblico una differenziazione analoga sta avendo luogo nell'ambito del decentramento o della separazione dei servizi politici e delle agenzie esecutive. In entrambi i settori viene accordata sempre più importanza allo sviluppo di catene di prestazione di servizi o alla prestazione di servizi inter-organismi, e al ricorso al subappalto o all'esternalizzazione di servizi per beneficiare di specializzazione e di eventuali economie di scala. Il risultato è un proliferare di vari servizi, e i prestatori che li offrono non sempre si considerano responsabili o tenuti a rendere conto del proprio operato. In funzione delle scelte organizzative delle imprese (e dei loro appaltatori o subappaltatori), le banche dati rilevanti possono trovarsi in uno o più paesi nell'Unione europea o al di fuori.

Lo sviluppo delle tecnologie di informazione e comunicazione ("TIC") ha ampiamente facilitato questi cambiamenti organizzativi, e vi ha pure contribuito. L'esercizio di responsabilità a diversi livelli - spesso derivante dalla differenziazione organizzativa - richiede generalmente, e incentiva, un largo ricorso alle TIC. Lo sviluppo e la diffusione dei prodotti e servizi TIC porta inoltre, a sua volta, all'emergere di nuovi ruoli e responsabilità a pieno titolo che non sempre interagiscono chiaramente con le responsabilità già esistenti o in fieri negli organismi clienti. È quindi importante essere consapevoli delle differenze pertinenti e di chiarire le responsabilità qualora ciò si renda necessario. Genera questioni analoghe in materia di slittamento delle responsabilità anche l'introduzione della microtecnologia, come i chip RFID nei prodotti di consumo. D'altro lato, solleva nuove e complicate questioni l'uso del computing distribuito, in particolare il "cloud computing" e le "griglie". [8]

A complicare ulteriormente la situazione vi è poi il fattore globalizzazione. Quando la differenziazione organizzativa e lo sviluppo delle TIC coinvolgono molteplici ordinamenti, come spesso avviene con Internet, le questioni relative al diritto applicabile sorgono inevitabilmente non solo nell'UE o nel SEE, ma anche in relazione ai paesi terzi. Un esempio si riscontra nel settore dell'antidoping: l'Agenzia mondiale antidoping (AMA), con sede in Svizzera, dispone di una banca dati contenente informazioni sugli atleti (ADAMS) che è gestita dal Canada in cooperazione con organizzazioni nazionali antidoping in tutto il mondo. Il Gruppo di lavoro Articolo 29 ha indicato che in questo caso la ripartizione delle responsabilità e l'attribuzione della responsabilità del trattamento sollevano specifiche difficoltà. [9]

Ciò significa che le questioni centrali esaminate nel presente parere hanno un grado elevato di rilevanza pratica e possono avere importanti conseguenze.

II.3. Sfide principali

Nell'ottica degli obiettivi della direttiva, è fondamentale garantire che la responsabilità del trattamento dei dati sia chiaramente definita e possa essere effettivamente applicata.

Se non è abbastanza chiaro chi deve fare cosa - ad es. se non è responsabile nessuno, o se vi sono molteplici potenziali responsabili -, vi è un ovvio rischio che succeda ben poco, se non addirittura niente, e che le disposizioni giuridiche rimangano lettera morta. Può anche succedere che interpretazioni ambigue portino a rivendicazioni contrastanti e ad altre controversie, nel qual caso gli effetti positivi sarebbero inferiori alle aspettative o potrebbero essere ridotti o neutralizzati da impreviste conseguenze negative.

In tutte queste situazioni, la sfida fondamentale consiste quindi nel fare sufficiente chiarezza per consentire e garantire un'efficace applicazione e osservanza nella pratica delle norme sulla protezione dei dati. In caso di dubbio, potrebbe essere privilegiata la soluzione più atta a sortire tali effetti.

Tuttavia, quegli stessi criteri che apportano sufficiente chiarezza possono anche generare complessità aggiuntive e conseguenze indesiderate. La differenziazione del controllo, ad esempio, nel contesto delle attuali realtà organizzative, può complicare la questione del diritto nazionale applicabile qualora siano coinvolte varie giurisdizioni.

Occorre quindi soppesare attentamente in che misura siano accettabili le conseguenze derivanti dalle disposizioni attuali, e l'eventuale necessità, invece, di un adeguamento delle norme vigenti per mantenerne l'efficacia ed evitare conseguenze inopportune derivanti da un cambiamento delle circostanze.

La presente analisi riveste quindi una grande importanza strategica e va applicata con cautela e nella piena consapevolezza di possibili interrelazioni fra i vari aspetti.

[4] Non viene utilizzato in nessuna delle disposizioni sostanziali, eccezion fatta per l'articolo 8, lettera a), in relazione al diritto di essere informati (principio di trasparenza). Il responsabile del casellario, come parte responsabile, appare solo in alcune parti della relazione.

[5] Cfr. anche il considerando 25 della [direttiva 95/46/CE](#): "Considerando che i principi di tutela si esprimono, da un lato, nei vari obblighi a carico delle persone, autorità pubbliche, imprese, agenzie o altri organismi responsabili del trattamento, obblighi relativi in particolare alla qualità dei dati, alla sicurezza tecnica, alla notificazione all'autorità di controllo, alle circostanze in cui il trattamento può essere effettuato e, dall'altro, nel diritto delle persone, i cui dati sono oggetto di trattamento, di esserne informate, di poter accedere ai dati, e chiederne la rettifica, o di opporsi al trattamento in talune circostanze."

[6] Il Gruppo di lavoro intende adottare un altro parere sul "diritto applicabile" nel corso del 2010. Quando le istituzioni e gli organismi comunitari trattano dati personali, la valutazione della responsabilità è rilevante anche ai fini della possibile applicazione del [regolamento \(CE\) 45/2001](#) o di altri strumenti giuridici pertinenti dell'Unione europea.

[7] Cfr. l'articolo 17, paragrafo 3, secondo trattino, che prevede che: "gli obblighi [...], quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incarico del trattamento, vincolino anche quest'ultimo".

[8] Il "cloud computing" ("nebulosa informatica") fornisce, come servizio, capacità informatiche scalabili ed elastiche a molteplici clienti che utilizzano tecnologie basate su Internet. Tipici servizi di cloud computing sono l'offerta di applicazioni aziendali on-line accessibili da un web browser, mentre il software e i dati sono conservati sui server. In tal senso, la "nebulosa" non è un'isola, ma un connettore globale di informazioni e utenti mondiali. Per quanto riguarda le "griglie", cfr. in appresso l'esempio 19.

[9] Parere 3/2008 del 1° agosto 2008 sul progetto di standard internazionale del codice mondiale antidoping per la protezione della privacy, WP156.

III. Analisi delle definizioni

III.1. Definizione di "responsabile del trattamento"

La definizione di "responsabile del trattamento" contenuta nella direttiva si articola intorno a tre componenti principali, che saranno analizzate separatamente ai fini del presente parere. Si tratta delle seguenti componenti:

- "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo"
- "che, da solo o insieme ad altri,"
- "determina le finalità e gli strumenti del trattamento di dati personali".

La prima componente riguarda il soggetto della definizione. La terza componente menziona gli aspetti essenziali per distinguere il responsabile del trattamento da altri attori. La seconda componente esamina la possibilità di una "responsabilità plurima". Benché queste componenti siano strettamente collegate, la metodologia seguita nel presente parere sarà di analizzarle separatamente.

A fini pratici, conviene cominciare col primo elemento della terza componente (cioè il significato della parola "determina"), continuare col resto della terza componente e solo in seguito esaminare la prima e la seconda componente.

III.1.a) Primo elemento: "determina"

Come già precedentemente indicato, il concetto di "responsabile" (controller) riveste nella Convenzione 108 minore importanza. Ai sensi dell'articolo 2 della Convenzione, il "responsabile del casellario" è definito come l'istanza "competente [...] a decidere". La Convenzione sottolinea la necessità della competenza, determinata "secondo il diritto nazionale", e rinvia così alle norme nazionali sulla protezione dei dati che, secondo la relazione, conterrebbero "criteri precisi" per stabilire chi è la persona competente.

Mentre la prima proposta della Commissione rispecchia questa disposizione, la proposta modificata si riferisce invece all'organismo che "decide", eliminando così la necessità che la competenza a decidere sia stabilita per legge: la definizione per legge è sempre possibile ma non necessaria. Ciò si vede poi confermato dalla posizione comune del Consiglio e dal testo adottato, che si riferiscono entrambi all'organismo "che determina".

In tale contesto, l'evoluzione storica della direttiva mette in evidenza due elementi importanti: in primo luogo, che è possibile essere responsabile del trattamento a prescindere da una specifica competenza o facoltà di controllare dati conferita per legge; in secondo luogo, che nel processo di adozione della direttiva 95/46 la determinazione del responsabile del trattamento diventa un concetto comunitario, che riveste un proprio significato indipendente nel diritto comunitario e non varia in funzione di disposizioni di diritto nazionale e delle loro eventuali divergenze. Quest'ultimo aspetto è fondamentale per garantire un'efficace applicazione della direttiva e un elevato livello di protezione negli Stati membri, che richiede un'interpretazione uniforme e quindi autonoma di un concetto tanto centrale quanto quello di "responsabile del trattamento" - che, come abbiamo visto, acquisisce nella direttiva un'importanza che non aveva nella Convenzione 108.

In tale ottica, la direttiva completa questa evoluzione stabilendo che, anche se la competenza a "determinare" può derivare da una specifica attribuzione per legge, ciò avverrebbe comunque generalmente in funzione degli elementi fattuali o delle circostanze del caso: occorre esaminare gli specifici trattamenti in questione e capire chi li determina, rispondendo inizialmente alle seguenti domande: "Qual è la ragione del trattamento? Chi l'ha iniziato?".

Essere il responsabile del trattamento deriva in primo luogo dal fatto concreto che un'entità ha scelto di trattare dati personali per propri fini. Un criterio puramente formale non sarebbe sufficiente almeno per due ragioni: in alcuni casi la designazione ufficiale di un responsabile del trattamento - prevista ad

esempio per legge, in un contratto o in una notificazione al garante per la protezione dei dati - verrebbe semplicemente a mancare; in altri casi, tale designazione ufficiale potrebbe non rispecchiare la realtà, conferendo il ruolo di responsabile del trattamento a un organismo che di fatto non è nella posizione di "determinare".

La pertinenza dell'influenza effettiva emerge anche dal caso SWIFT [10], in cui la SWIFT era formalmente considerata l'incaricato del trattamento dei dati, ma di fatto agiva - almeno entro una certa misura - come responsabile del trattamento. In quel caso è stato chiarito che, benché la designazione di una parte come responsabile o incaricato del trattamento in un contratto possa fornire informazioni rilevanti sullo status giuridico della parte, una tale designazione contrattuale non permette tuttavia di stabilirne in modo definitivo lo status effettivo, che deve essere basato su circostanze concrete.

Questo approccio fattuale è avallato anche dalla direttiva stessa, che stabilisce che il responsabile del trattamento è l'organismo che "determina", e non che "determina lecitamente" la finalità e gli strumenti del trattamento. L'individuazione effettiva della responsabilità del trattamento è decisiva anche se la designazione si rivela illecita o se illecito è il modo in cui è effettuato il trattamento dei dati. Non importa se la decisione di trattare i dati è "lecita" nel senso che l'entità che l'ha presa è giuridicamente atta a farlo, o nel senso che un responsabile del trattamento è stato ufficialmente nominato secondo una specifica procedura. La questione della liceità del trattamento dei dati personali interverrà in un secondo tempo e sarà valutata alla luce degli altri articoli della direttiva (in particolare gli articoli 6-8). In altri termini, è importante garantire che, anche nei casi in cui i dati sono trattati illecitamente, un responsabile del trattamento possa essere facilmente individuato e risponda del trattamento in questione.

Un'ultima peculiarità del concetto di responsabile del trattamento è la sua autonomia, nel senso che, anche se fonti giuridiche esterne possono aiutare ad identificare tale figura, il concetto va interpretato principalmente alla luce delle disposizioni relative alla protezione dei dati. [11] La nozione di responsabile del trattamento non va confusa con altri concetti - a volte confliggenti o sovrapposti - di altri settori del diritto (ad es. il creatore o il titolare del diritto nel settore della proprietà intellettuale). Essere un titolare di un diritto di proprietà intellettuale non esclude la possibilità di poter essere anche un "responsabile del trattamento" e di essere quindi soggetto agli obblighi derivanti dalle disposizioni relative alla protezione dei dati.

Necessità di una tipologia

Il concetto di responsabile del trattamento è funzionale, finalizzato cioè all'attribuzione di responsabilità laddove intervenga un'influenza effettiva: si basa quindi su un'analisi fattuale piuttosto che formale. Per stabilire chi esercita tale responsabilità può quindi essere talvolta necessaria un'indagine lunga e approfondita. Tuttavia, la necessità di garantire un'efficace protezione dei dati richiede un approccio pragmatico per assicurare la prevedibilità per quanto riguarda la responsabilità. In tale ottica si rendono necessarie norme empiriche e presunzioni d'ordine pratico per guidare e semplificare l'applicazione delle norme relative alla protezione dei dati.

Ciò richiede un'interpretazione della direttiva che garantisca che "l'organismo che determina" possa essere facilmente e chiaramente identificato nella maggior parte delle situazioni, facendo riferimento a quelle circostanze - giuridiche e/o fattuali - da cui è generalmente possibile inferire un'influenza effettiva, salvo indicazione contraria.

Tali circostanze possono essere analizzate e classificate in base alle tre categorie di situazioni esposte in appresso, che consentono un approccio sistematico alle questioni in oggetto.

1) Responsabilità derivante da un'esplicita competenza giuridica. A questa situazione, fra l'altro, si riferisce la seconda parte della definizione, che menziona il caso in cui il responsabile del trattamento o i criteri specifici per la sua designazione sono fissati dal diritto nazionale o comunitario. L'esplicita designazione del responsabile del trattamento per legge non è frequente e non presenta generalmente

grossi problemi. In alcuni paesi, la legislazione nazionale prevede che le pubbliche autorità siano responsabili del trattamento dei dati personali nell'ambito delle loro funzioni.

Accade tuttavia più frequentemente che la legge, invece che designare direttamente il responsabile del trattamento o definire i criteri di una tale designazione, affidi il compito, o imponga l'obbligo, a qualcuno, di raccogliere e trattare certi dati. Potrebbe ad esempio essere il caso di un ente cui sono affidate mansioni pubbliche (ad es. la sicurezza sociale) che non possono essere assolte senza raccogliere almeno una serie di dati personali, e che crea quindi, a tal fine, un apposito registro. In tal caso, è dalla legge che discende chi è il responsabile del trattamento. Più in generale, la legge può obbligare organismi pubblici o privati a conservare o fornire certi dati: questi organismi dovrebbero allora, in linea generale, essere considerati i responsabili di qualunque trattamento dei dati personali in tale contesto.

2) Responsabilità derivante da una competenza implicita. È il caso in cui la competenza a determinare non è esplicitamente stabilita per legge né discende direttamente da esplicite disposizioni giuridiche, ma deriva da disposizioni giuridiche comuni o da una prassi giuridica consolidata in diversi settori (diritto civile, diritto commerciale, diritto del lavoro, ecc.). In tal caso i ruoli tradizionali esistenti, di una certa responsabilità, potranno aiutare ad individuare il responsabile del trattamento: ad es. il datore di lavoro per i dati dei suoi dipendenti, l'editore per i dati dei suoi abbonati, l'associazione per i dati dei suoi membri o sottoscrittori.

In tutti questi casi, la competenza a determinare attività di trattamento può essere considerata naturalmente collegata al ruolo funzionale di un'organizzazione (privata), che comporta in definitiva delle responsabilità anche sul piano della protezione dei dati. Da un punto di vista giuridico ciò varrebbe indipendentemente dal fatto che la capacità di determinazione sia conferita alle menzionate persone giuridiche, sia esercitata da appositi organi che agiscono per loro conto, o da una persona fisica con un ruolo analogo (si veda, in appresso, la disamina del primo elemento, punto c)). Lo stesso varrebbe comunque per un'autorità pubblica con determinati compiti amministrativi, in un paese in cui la legge non contenga esplicite disposizioni quanto alla responsabilità in materia di protezione dei dati.

Esempio n. 1: Operatori di telecomunicazione

Un interessante esempio di orientamenti giuridici per il settore privato riguarda il ruolo degli operatori di telecomunicazione. Il considerando 47 della direttiva 95/46/CE precisa che " laddove un messaggio contenente dati personali sia trasmesso tramite un servizio di telecomunicazioni o di posta elettronica, finalizzato unicamente alla trasmissione di siffatti messaggi, si considera, di norma, responsabile del trattamento dei dati personali contenuti del messaggio la persona che lo ha emanato e non la persona che presta il servizio di trasmissione; [...] tuttavia le persone che prestano tali servizi sono di norma considerate responsabili del trattamento dei dati personali supplementari necessari per il funzionamento del servizio". Il fornitore di servizi di telecomunicazione dovrebbe quindi, in linea di principio, essere considerato responsabile del trattamento solo per i dati relativi al traffico e alla fatturazione, e non per i dati trasmessi [12]. Questo orientamento giuridico del legislatore comunitario è assolutamente in linea con l'approccio funzionale seguito nel presente parere.

3) Responsabilità derivante da un'influenza effettiva. È il caso in cui la responsabilità del trattamento viene attribuita in base ad una valutazione delle circostanze di fatto. In molti casi ciò comporterà una valutazione delle relazioni contrattuali fra le varie parti interessate, che consentirà di trarre conclusioni, dall'esterno, sull'attribuzione del ruolo di responsabile del trattamento e dei relativi obblighi ad una o più di tali parti. Ciò può essere di particolare utilità in contesti complessi, in cui si ricorre spesso alle nuove tecnologie dell'informazione, e in cui gli attori rilevanti tendono a considerarsi dei "mediatori" e non i responsabili del trattamento.

Può accadere che un contratto non indichi chi è il responsabile del trattamento, ma contenga elementi sufficienti per assegnare tale qualifica a una parte che risulta esercitare un ruolo dominante. Può anche accadere che il contratto sia più esplicito quanto alla designazione del responsabile del

trattamento: se non vi sono ragioni di dubitare che le clausole interessate non rispecchino accuratamente la realtà dei fatti, nulla impedisce di applicare le condizioni del contratto. Tuttavia, le clausole di un contratto non sono sempre decisive, poiché ciò consentirebbe alle parti di assegnare le responsabilità nel modo per loro più conveniente.

Il fatto stesso che qualcuno determini le modalità del trattamento dei dati personali può far scattare la qualifica di responsabile del trattamento, anche se al di fuori dell'ambito di una relazione contrattuale o anche se esplicitamente esclusa dal contratto. Un chiaro esempio è il caso SWIFT, in cui la società ha deciso di rendere disponibili alcuni dati personali (originariamente trattati a fini commerciali per conto di istituti finanziari) anche ai fini della lotta contro il finanziamento del terrorismo, come richiesto ufficialmente dal Tesoro statunitense.

In caso di dubbio, per individuare il responsabile del trattamento si possono esaminare anche altri elementi extracontrattuali, come il grado di controllo reale esercitato da una parte, l'immagine data agli interessati e il legittimo affidamento di questi ultimi sulla base di questa visibilità (si veda anche, in appresso, la disamina del terzo elemento, punto b)). Questa categoria è particolarmente importante poiché consente di esaminare e di attribuire responsabilità anche nei casi di comportamento illecito, in cui le attività di trattamento possono anche essere svolte contro gli interessi e la volontà di alcune delle parti.

Conclusioni preliminari

Di queste categorie, le prime due consentono in linea di principio di individuare con maggior sicurezza l'"organismo che determina", e possono applicarsi in pratica a più dell'80% delle situazioni rilevanti. Tuttavia, una designazione giuridica ufficiale dovrebbe essere conforme alle norme relative alla protezione dei dati, garantendo che l'organismo nominato abbia il controllo effettivo dei trattamenti, o, in altre parole, che la designazione giuridica rispecchi la realtà della situazione.

La categoria 3 richiede un'analisi più complessa e può più facilmente portare ad interpretazioni divergenti. Le condizioni di un contratto possono spesso aiutare a chiarire la questione, ma non sono sempre decisive. Vi è un numero crescente di attori che ritengono di non essere loro a determinare le attività di trattamento, e che non si considerano quindi responsabili. In tali casi l'unica opzione praticabile è trarre una conclusione in base all'influenza effettiva. La questione della liceità del trattamento sarà valutata alla luce degli altri articoli della direttiva (in particolare gli articoli 6-8).

Se nessuna delle categorie di cui sopra è applicabile, la designazione di un responsabile del trattamento dovrà essere considerata "nulla": un organismo che non ha un'influenza, né giuridica né di fatto, per determinare le modalità del trattamento dei dati non può in effetti essere considerato il responsabile del trattamento.

Da un punto di vista formale, questo approccio è corroborato dalla considerazione che la definizione di responsabile del trattamento dovrebbe essere ritenuta come una disposizione giuridica obbligatoria cui le parti non possono derogare e che non possono aggirare. Da un punto di vista strategico, una tale designazione sarebbe contraria a un'efficace applicazione delle norme sulla protezione dei dati e invaliderebbe l'esercizio della responsabilità che comporta il trattamento dei dati.

III.1.b) Terzo elemento: "finalità e strumenti del trattamento"

Il terzo elemento rappresenta la parte sostanziale del testo: cosa deve determinare una parte per essere qualificata come responsabile del trattamento.

L'iter di questa disposizione è caratterizzato da numerose evoluzioni. La Convenzione 108 si riferiva alla finalità del casellario automatizzato, alle categorie di dati a carattere personale e alle operazioni ad essi applicabili. La Commissione ha mutuato questi elementi sostanziali modificandone leggermente la formulazione, e ha aggiunto la facoltà di decidere quali parti terze possano avere accesso ai dati. La proposta modificata della Commissione ha fatto un passo avanti passando da "la finalità dell'archivio"

a "le finalità e gli obiettivi del trattamento", e slittando così da una definizione statica, associata a un casellario, ad una definizione dinamica associata all'attività di trattamento. La proposta modificata si riferiva sempre a quattro elementi (finalità/obiettivi, dati personali, operazioni e terzi aventi accesso), ridotti a due ("finalità e strumenti") solo dalla posizione comune del Consiglio.

I dizionari definiscono la "finalità" come un risultato sperato, che si persegue o che guida le azioni previste, e lo "strumento" come il modo di ottenere un risultato o di raggiungere un fine.

La direttiva stabilisce che i dati devono essere rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. La determinazione delle "finalità" del trattamento e degli "strumenti" per raggiungerle è quindi di somma importanza.

Si può anche dire che determinare le finalità e gli strumenti equivale a determinare, rispettivamente, il "perché" e il "come" di certe attività di trattamento. In tale ottica, e tenendo conto del fatto che questi due elementi sono collegati, sorge la necessità di dare degli orientamenti sul livello di influenza su tale "perché" e su tale "come" che può far scattare la qualificazione di un'entità come responsabile del trattamento.

Nel valutare la determinazione delle finalità e degli strumenti per attribuire il ruolo di responsabile del trattamento, la domanda centrale che sorge è quindi quanto dettagliatamente occorra determinare tali finalità e strumenti per poter essere considerati responsabili del trattamento. E, collegata a tale domanda, qual è il marginale di manovra lasciato dalla direttiva all'incaricato del trattamento. Queste definizioni diventano particolarmente rilevanti quando nel trattamento di dati personali sono implicate diverse figure, ed è necessario stabilire chi sono i responsabili del trattamento (da soli o insieme ad altri) e chi sono invece, se del caso, gli incaricati del trattamento.

L'importanza da accordare alle finalità o agli strumenti può variare a seconda dello specifico contesto in cui ha luogo il trattamento.

È necessario un approccio pragmatico, che privilegi la discrezionalità nel determinare le finalità e il margine di manovra nell'adozione delle decisioni. In questi casi, la domanda che sorge è perché ha luogo il trattamento e qual è il ruolo delle figure eventualmente implicate, come le società di esternalizzazione: la società esternalizzata avrebbe trattato i dati se il responsabile del trattamento non gliel'avesse chiesto, e a quali condizioni? Un incaricato del trattamento potrebbe, poi, seguire gli orientamenti generali dati principalmente sulle finalità senza entrare veramente nei dettagli per quanto riguarda gli strumenti.

Esempio n. 2: Marketing via e-mail

La società ABC stipula contratti con varie organismi per effettuare le sue campagne di marketing via e-mail e per gestire le buste paga, dando chiare istruzioni (quale materiale promozionale diramare e a chi, e chi pagare, quali importi, a quale data, ecc.). Benché gli organismi abbiano un certo margine di manovra (anche quanto al software da utilizzare), i loro compiti sono chiaramente e rigorosamente definiti, e, anche se possono ricevere consigli dalla società di mailing (che può raccomandare, ad es., di non inviare mail in agosto), sono chiaramente tenuti ad agire secondo le istruzioni di ABC. Inoltre, solo un'entità, cioè la società ABC, ha il diritto di utilizzare i dati trattati - tutte le altre entità devono richiamarsi alla base giuridica della società ABC se viene chiamata in causa la loro facoltà di trattare i dati. In questo caso è chiaro che la società ABC è il responsabile del trattamento e che ognuno dei singoli organismi può essere considerato come un incaricato del trattamento riguardo allo specifico trattamento di dati effettuato per conto del responsabile.

Per quanto riguarda la determinazione degli strumenti, va detto innanzitutto che il termine "strumenti" comprende evidentemente vari tipi di elementi, come emerge peraltro anche dall'iter di questa definizione. Nella proposta originaria, il ruolo del responsabile del trattamento deriverebbe dal determinare quattro elementi (finalità/obiettivo, dati personali, operazioni e terzi aventi accesso). La formulazione finale della disposizione, che si riferisce solo a "finalità e strumenti" non può essere considerata in contraddizione con la versione anteriore, poiché non vi può essere alcun dubbio sul

fatto, ad es., che il responsabile del trattamento debba determinare quali dati debbano essere trattati per la finalità o le finalità previste. Pertanto, la definizione finale deve essere interpretata piuttosto solo come una versione abbreviata che conserva comunque il senso della versione anteriore. In altri termini, "strumenti" non si riferisce solo ai mezzi tecnici per trattare i dati personali, ma anche al "come" del trattamento, cioè "quali dati saranno trattati", "quali terzi avranno accesso ai dati", "quando tali dati saranno eliminati", ecc.

La determinazione degli "strumenti" ingloba quindi questioni sia tecniche che organizzative la cui decisione può anche essere delegata agli incaricati del trattamento (ad es. "quale hardware o software utilizzare?"), nonché elementi essenziali tradizionalmente e intrinsecamente riservati al responsabile del trattamento, come "quali dati trattare?", "per quanto tempo trattarli?", "chi vi ha accesso?", e così via.

In questo contesto, mentre la determinazione della finalità del trattamento farebbe scattare in ogni caso la qualifica di responsabile del trattamento, la determinazione dei mezzi implicherebbe una responsabilità solo qualora riguardi gli aspetti fondamentali dei mezzi.

In tale ottica, è del tutto possibile che i mezzi tecnici ed organizzativi siano determinati esclusivamente dall'incaricato del trattamento.

In questi casi - quando le finalità sono chiaramente definite, ma vi sono pochi orientamenti, se non nessuno, quanto ai mezzi tecnici ed organizzativi - gli strumenti dovrebbero rappresentare una ragionevole via per realizzare la o le finalità perseguite e il responsabile del trattamento dei dati dovrebbe essere pienamente informato in merito. Se un contraente influisce sulla finalità del trattamento e lo effettua (anche) a proprio beneficio - usando ad esempio, i dati personali ricevuti per generare servizi a valore aggiunto -, si renderebbe allora responsabile (o eventualmente corresponsabile) del trattamento per un'altra attività di trattamento, e sarebbe quindi soggetto a tutti gli obblighi della normativa applicabile in materia di protezione dei dati.

Esempio n. 3: La società designata come incaricato del trattamento agisce come responsabile del trattamento

La società MarketinZ fornisce servizi di pubblicità promozionale e marketing diretto a varie imprese. La società GoodProductZ conclude un contratto con MarketinZ: in base a tale contratto MarketinZ fornisce servizi di pubblicità commerciale per i clienti di GoodProductZ ed è designata come incaricato del trattamento. MarketinZ, tuttavia, decide di usare la banca dati dei clienti di GoodProducts per promuovere prodotti anche di altri clienti. Questa decisione, di aggiungere un'altra finalità a quella per cui erano stati inizialmente trasmessi i dati personali, fa di MarketinZ il responsabile del trattamento per tale operazione. La questione della liceità di tale trattamento sarà valutata alla luce di altri articoli (6-8).

In alcuni ordinamenti giuridici le decisioni prese in merito alle misure di sicurezza sono particolarmente importanti, poiché sono esplicitamente considerate come un peculiare aspetto che deve essere definito dal responsabile del trattamento. Ci si chiede quindi quali decisioni in materia di sicurezza possono far scattare la qualifica di responsabile del trattamento per una società a cui è stata esternalizzata l'elaborazione dei dati.

Conclusioni preliminari

La determinazione della "finalità" del trattamento è riservata al "responsabile del trattamento". Chiunque prenda questa decisione è quindi (di fatto) il responsabile del trattamento. Questi può a sua volta delegare la determinazione degli "strumenti" del trattamento per quanto riguarda le questioni tecniche od organizzative. Le questioni sostanziali, attinenti ai fondamenti della liceità del trattamento, sono riservate al responsabile. Una persona o un'entità che decida, ad es., per quanto tempo debbano essere conservati i dati elaborati o chi vi avrà accesso, agisce come "responsabile" per tale parte dell'uso dei dati, e deve quindi ottemperare a tutti gli obblighi che incombono al responsabile del trattamento.

III.1.c) Primo elemento: "persona fisica, persona giuridica o qualsiasi altro organismo"

Il primo elemento della definizione si riferisce al soggetto: chi può essere il responsabile del trattamento, e rispondere così in definitiva degli obblighi derivanti dalla direttiva. La definizione rispecchia esattamente la formulazione dell'articolo 2 della Convenzione 108 e non ha dato adito a specifici dibattiti nel corso del processo decisionale relativo alla direttiva. Si riferisce a una vasta gamma di soggetti che possono svolgere il ruolo di responsabile del trattamento, dalla persona fisica alla persona giuridica, includendo "qualsiasi altro organismo".

È importante che l'interpretazione di questo elemento garantisca un'efficace applicazione della direttiva favorendo il più possibile una chiara e univoca identificazione del responsabile del trattamento in tutte le circostanze, indipendentemente dal fatto che si sia proceduto o meno a una designazione ufficiale e che tale designazione sia stata resa pubblica.

In primo luogo, è importante attenersi il più possibile alla prassi stabilita sia nel settore pubblico che in quello privato da altri ambiti del diritto, come quello civile, amministrativo e penale. Nella maggior parte dei casi queste disposizioni indicheranno a quali persone od organismi vanno attribuite le responsabilità, e aiuteranno in linea di principio a individuare chi è il responsabile del trattamento.

Nell'ottica strategica dell'attribuzione delle responsabilità, e per dare agli interessati un'entità di riferimento più stabile e più affidabile per l'esercizio dei loro diritti ai sensi della direttiva, sarebbe preferibile considerare come responsabile del trattamento la società o l'organismo in quanto tali piuttosto che una specifica persona al loro interno. Sono la società o l'organismo a dovere, in ultima analisi, essere considerati responsabili del trattamento dei dati e degli obblighi derivanti dalla normativa sulla protezione dei dati, a meno che non vi siano elementi chiari che indichino che a rispondere di ciò sia una persona fisica. In generale, occorre presupporre che la società o l'organismo pubblico siano responsabili in quanto tali dei trattamenti che avvengono nel loro ambito di attività e di rischi.

Talvolta, le società e gli organismi pubblici designano una persona specifica come responsabile dell'attuazione dei trattamenti. Tuttavia, anche nel caso in cui una specifica persona fisica sia nominata per garantire il rispetto dei principi di protezione dei dati o per trattare dati personali, tale persona non sarà il responsabile del trattamento ma agirà per conto della persona giuridica (società od organismo pubblico) che risponderà, in qualità di responsabile del trattamento, in caso di violazione.

[13]

Si tratta, specialmente per le strutture grosse e complesse, di una questione fondamentale di "governance della protezione dei dati", che garantisce al tempo stesso una chiara responsabilità della persona fisica che rappresenta la società e concrete responsabilità funzionali all'interno della struttura, ad esempio incaricando altre persone di intervenire come rappresentanti o referenti per gli interessati.

Una particolare analisi si rende necessaria nei casi in cui una persona fisica che opera all'interno di una persona giuridica utilizzi dati per propri scopi al di fuori dell'ambito e del possibile controllo delle attività della persona giuridica. In questo caso la persona fisica interessata sarebbe il responsabile del trattamento deciso, e risponderebbe di questo utilizzo di dati personali. Il responsabile del trattamento originario potrebbe comunque conservare una certa responsabilità nel caso in cui il nuovo trattamento fosse dovuto a una mancanza di adeguate misure di sicurezza.

Come già sopra menzionato, il ruolo del responsabile del trattamento è fondamentale e particolarmente rilevante quando si tratta di determinare la responsabilità e di infliggere sanzioni. Anche se la responsabilità e le sanzioni varieranno da uno Stato membro all'altro in quanto stabilite dal diritto nazionale, la necessità di individuare chiaramente la persona fisica o giuridica responsabile di eventuali violazioni della normativa sulla protezione dei dati è senz'ombra di dubbio un presupposto essenziale per un'efficace applicazione della direttiva.

L'identificazione del "responsabile del trattamento", nell'ottica della protezione dei dati, sarà collegata in pratica alle norme di diritto civile, amministrativo o penale che disciplinano l'attribuzione delle responsabilità o l'imposizione di sanzioni cui può essere soggetta una persona giuridica o fisica [14].

La responsabilità civile non dovrebbe sollevare specifiche questioni nel presente contesto, poiché si applica sia alle persone giuridiche che alle persone fisiche. La responsabilità penale/o amministrativa, tuttavia, può, in funzione del diritto nazionale, applicarsi solo alle persone fisiche. Se il diritto nazionale prevede sanzioni penali o amministrative per violazioni delle norme sulla protezione dei dati, lo stesso diritto stabilirà anche chi è responsabile: se la responsabilità penale o amministrativa delle persone giuridiche non è riconosciuta, essa può essere riversata sui dipendenti delle persone giuridiche in virtù di speciali disposizioni del diritto nazionale [15].

Il diritto europeo contiene utili esempi di criteri di attribuzione della responsabilità penale [16], in particolare quando un reato è commesso a vantaggio della persona giuridica. In tal caso può essere considerato responsabile qualsiasi soggetto "che detenga una posizione preminente in seno alla persona giuridica, individualmente o in quanto parte di un organo della persona giuridica, in virtù:

- (a) del potere di rappresentanza della persona giuridica;
- (b) del potere di prendere decisioni per conto della persona giuridica; o;
- (c) del potere di esercitare un controllo in seno alla persona giuridica."

Conclusioni preliminari

Sintetizzando le riflessioni di cui sopra, si può concludere che la persona che risponde delle violazioni delle norme sulla protezione dei dati è sempre il responsabile del trattamento, cioè la persona giuridica (società od organismo pubblico) o la persona fisica quale formalmente identificata secondo i criteri della direttiva. Se una persona fisica che lavora in una società o in un organismo pubblico usa dei dati per scopi propri al di fuori delle attività della società, tale persona sarà considerata come il responsabile del trattamento di fatto e dovrà rispondere in quanto tale.

Esempio n. 4: Controllo segreto dei dipendenti

Un membro del consiglio d'amministrazione di una società decide di controllare segretamente i dipendenti dell'impresa, anche se tale decisione non è ufficialmente approvata dal consiglio d'amministrazione. La società deve essere considerata come il responsabile del trattamento e deve far fronte agli eventuali ricorsi dei dipendenti i cui dati siano stati oggetto di utilizzo abusivo, nonché rispondere di ciò.

La responsabilità della società deriva in particolare dal fatto che, in quanto responsabile del trattamento, è tenuta a garantire l'osservanza delle disposizioni in materia di sicurezza e riservatezza. Un utilizzo abusivo dei dati da parte di un dirigente dell'impresa o di un dipendente potrebbe essere considerato come la conseguenza di misure di sicurezza inadeguate. Tutto questo indipendentemente dal fatto che, in una fase ulteriore, anche il membro del consiglio d'amministrazione o altre persone fisiche all'interno della società possano essere considerate responsabili, sia civilmente - anche nei confronti dell'impresa -, sia penalmente. Ciò potrebbe accadere ad esempio se il membro del consiglio d'amministrazione usasse i dati raccolti per ottenere favori personali dai dipendenti: dovrebbe allora essere considerato come "responsabile del trattamento" e rispondere di questo specifico utilizzo dei dati.

III.1.d) Secondo elemento: "da solo o insieme ad altri"

Il presente paragrafo, basandosi sulla precedente analisi delle peculiarità del responsabile del trattamento, esaminerà i casi in cui il trattamento di dati personali veda interagire più figure. Vi è in effetti un numero crescente di casi in cui vari soggetti agiscono come responsabili del trattamento - e la definizione della direttiva lo prevede.

La possibilità che il responsabile del trattamento operi "da solo o insieme ad altri" non figurava nella Convenzione 108, ed è stata introdotta dal Parlamento europeo prima dell'adozione della direttiva. Nel

parere della Commissione sugli emendamenti del Parlamento europeo, la Commissione si riferisce alla possibilità che, "per uno stesso trattamento, possono esservi più corresponsabili che determinano assieme la finalità del trattamento e gli strumenti da utilizzare per effettuarlo", e di conseguenza che, in tal caso, "ciascuno dei corresponsabili deve considerarsi tenuto al rispetto delle obbligazioni poste dalla presente direttiva al fine di proteggere le persone fisiche i dati delle quali sono trattati".

Il parere della Commissione non rispecchia del tutto la complessità della realtà attuale in materia di protezione dei dati, poiché riguarda solo il caso in cui tutti i responsabili del trattamento determinano in uguale misura uno stesso trattamento e in uguale misura ne rispondono. La realtà mostra invece che questo è solo uno dei vari tipi di "responsabilità plurima" che possono esistere. In tale ottica, l'espressione "insieme a" deve essere interpretata come se significasse "non da solo", in varie forme e combinazioni.

In primo luogo, va osservato che la probabilità di vedere intervenire molteplici soggetti nell'elaborazione di dati personali è naturalmente collegata ai molteplici tipi di attività che secondo la direttiva possono essere considerati come il "trattamento", che è in definitiva l'oggetto della "corresponsabilità". La definizione di "trattamento" di cui all'articolo 2, lettera b) della direttiva non esclude la possibilità che diversi attori intervengano in varie operazioni o insiemi di operazioni su dati personali, che possono avere luogo simultaneamente o in varie fasi.

In un contesto così complesso è ancora più importante che i ruoli e le responsabilità possano essere facilmente attribuiti, per garantire che la complessità della corresponsabilità non porti ad un'impraticabile ripartizione delle responsabilità che minerebbe l'efficacia della normativa sulla protezione dei dati. La molteplicità delle possibili configurazioni non permette tuttavia di stabilire un elenco esaustivo e "chiuso" o una classificazione dei vari tipi di "corresponsabilità". È comunque utile fornire anche a tale riguardo degli orientamenti, definendo alcune categorie e dando alcuni esempi di corresponsabilità, insieme ad elementi fattuali da cui la corresponsabilità può essere inferita o presupposta.

In generale, l'analisi della corresponsabilità deve rispecchiare quella della responsabilità "singola" sviluppata sopra, nei paragrafi da III.1.a) a c). Analogamente, anche nella valutazione della corresponsabilità va seguito un approccio sostanziale e funzionale, come sopra illustrato, che valuti se le finalità e gli strumenti sono determinati da più di una parte.

Esempio n. 5: Installazione di telecamere di videosorveglianza

Il proprietario di un immobile stipula un contratto con una società di vigilanza, affinché questa installi delle telecamere in varie parti dell'edificio per conto del responsabile del trattamento. Le finalità della videosorveglianza e il modo in cui le immagini sono raccolte e conservate sono determinati esclusivamente dal proprietario dell'edificio, che quindi va considerato l'unico responsabile del trattamento per questa operazione.

Anche in questo contesto, degli accordi contrattuali possono essere utili ai fini della valutazione della corresponsabilità, ma occorrono sempre dei riscontri in base alle relazioni concrete fra le parti.

Esempio n. 6: Cacciatori di teste

La società Headhunterz Ltd aiuta Enterprize Inc ad assumere nuovo personale. Il contratto indica chiaramente che "Headhunterz Ltd agisce per conto di Enterprize e procede all'elaborazione dei dati personali in qualità di incaricato del trattamento. Enterprize è l'unico responsabile del trattamento dei dati". Headhunterz Ltd si trova tuttavia in una posizione ambigua: da un lato ha il ruolo di responsabile del trattamento nei confronti delle persone che cercano un impiego, dall'altro si impegna come incaricato del trattamento per conto dei responsabili del trattamento, quali Enterprize Inc e altre società che ricorrono ai suoi servizi di assunzione. Inoltre Headhunterz - con il suo famoso servizio a valore aggiunto "global matchz" - cerca candidati idonei sia in base ai CV ricevuti direttamente da Enterprize che in base a quelli che già possiede nella sua ampia banca dati. Ciò permette ad Headhunterz - che è remunerata solo per i contratti effettivamente firmati - di accrescere il tasso di incontro fra offerte e domande di lavoro, aumentando così le proprie entrate. In base a questi elementi si può affermare che, nonostante la qualifica contrattuale, Headhunterz Ltd debba essere considerata come un responsabile del trattamento, che risponde insieme a Enterprize Inc in ogni caso per quegli insiemi di operazioni relativi alle assunzioni per Enterprize.

In quest'ottica, si è in presenza di una situazione di corresponsabilità quando varie parti determinano, per specifici trattamenti, o la finalità o quegli aspetti fondamentali degli strumenti che caratterizzano il responsabile del trattamento (cfr. sopra, paragrafi da III.1.a) a c).

Nel contesto della corresponsabilità, comunque, la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale. In effetti, quando vi è una pluralità di attori, questi possono avere una relazione molto stretta (condividendo, ad esempio, tutte le finalità e tutti gli strumenti di un trattamento) o più distante (condividendo ad esempio solo le finalità o i mezzi, o una parte di essi). Va quindi esaminata un'ampia varietà di tipologie di corresponsabilità e ne vanno analizzate le rispettive conseguenze giuridiche, lasciando una certa flessibilità per tenere conto della crescente complessità della realtà attuale del trattamento dei dati.

In questo contesto, è necessario esaminare i vari gradi di interazione o di legame fra le diverse parti coinvolte nel trattamento dei dati personali.

In primo luogo, il mero fatto che diversi soggetti cooperino all'elaborazione di dati personali, ad esempio a catena, non significa necessariamente che siano sempre corresponsabili: in effetti uno scambio di dati fra due parti, senza che vi sia una condivisione di finalità o strumenti in un insieme di operazioni comuni, deve essere considerato un semplice trasferimento di dati fra due distinti responsabili del trattamento.

Esempio n. 7: Agenzia di viaggi (1)

Un'agenzia invia dati personali dei suoi clienti alle compagnie aeree e a una catena d'alberghi per effettuare delle prenotazioni per un pacchetto viaggi. La compagnia aerea e l'albergo confermano la disponibilità dei posti e delle camere richiesti. L'agenzia emette i documenti di viaggio e i voucher per i suoi clienti. In questo caso, l'agenzia di viaggi, la compagnia aerea e l'hotel saranno tre responsabili distinti, ciascuno soggetto agli obblighi di protezione dei dati in relazione al proprio trattamento.

La valutazione può tuttavia essere diversa se attori diversi decidono di creare un'infrastruttura comune per perseguire i loro fini personali. Quando, nel creare tale infrastruttura, questi attori determinano gli aspetti fondamentali degli strumenti da utilizzare, divengono, perlomeno in tale misura, corresponsabili del trattamento, anche se non condividono necessariamente le stesse finalità.

Esempio n. 8: Agenzia di viaggi (2)

L'agenzia, la catena alberghiera e la compagnia aerea decidono di creare una piattaforma comune su Internet per migliorare la loro cooperazione nella gestione delle prenotazioni. Concordano insieme aspetti importanti degli strumenti da utilizzare, ad es. quali dati saranno conservati, come saranno distribuite e confermate le prenotazioni, e chi potrà avere accesso alle informazioni conservate. Decidono inoltre di condividere i dati dei loro clienti per svolgere azioni integrate di marketing.

In questo caso l'agenzia di viaggi, la compagnia aerea e la catena alberghiera risponderanno congiuntamente del trattamento dei dati dei loro rispettivi clienti, e saranno così corresponsabili per quanto riguarda i trattamenti relativi alla piattaforma comune di prenotazione su Internet. Tuttavia, ciascuno di questi soggetti rimane responsabile individualmente per le altre attività di trattamento, ad es. quelle riguardanti la gestione delle proprie risorse umane.

Accade che vari attori trattino gli stessi dati personali in sequenza. In questi casi, a livello microscopico, i vari trattamenti della catena possono sembrare scollegati, come se ognuno avesse una finalità differente. È necessario tuttavia verificare se, a livello macroscopico, questi trattamenti non debbano invece essere considerati come un "insieme di operazioni" che perseguono una finalità comune o che si avvalgono di strumenti stabiliti congiuntamente.

I due esempi che seguono chiariscono questa idea proponendo due possibili scenari.

Esempio n. 9: Trasferimento di dati dei dipendenti all'amministrazione fiscale

La società XYZ raccoglie e tratta i dati personali dei suoi dipendenti per gestire gli stipendi, le missioni, le assicurazioni malattia, ecc. La società ha comunque anche l'obbligo di legge di inviare tutti i dati relativi agli stipendi all'amministrazione tributaria, per rafforzare il controllo fiscale.

In questo caso, anche se sia la società XYZ che le autorità fiscali trattano gli stessi dati relativi ai salari, l'assenza di finalità o strumenti comuni fa sì che le due entità siano due distinti responsabili del trattamento dei dati.

Esempio n. 10: Transazioni finanziarie

Prendiamo invece il caso di una banca che ricorre a un fornitore di servizi di messaggeria finanziaria per realizzare le sue transazioni finanziarie. La banca e il fornitore di servizi concordano gli strumenti di trattamento dei dati finanziari. I dati personali collegati alle transazioni finanziarie vengono in un primo tempo elaborati dall'istituto finanziario e solo in un secondo momento dal servizio di messaggeria. Anche se, a livello microscopico, ciascuno di questi soggetti persegue la propria finalità, a livello macroscopico le varie fasi e le finalità e gli strumenti del trattamento sono invece strettamente collegati. In questo caso, la banca e il fornitore di servizi di messaggeria finanziaria possono essere considerati corresponsabili del trattamento.

Vi sono anche casi in cui i vari attori coinvolti determinano insieme, a volte in misura diversa, le finalità e/o i mezzi di un trattamento.

A volte ogni responsabile risponde solo di una parte del trattamento, ma le informazioni vengono riunite ed elaborate attraverso una piattaforma.

Esempio n. 11: Portali amministrativi in rete

I portali amministrativi in rete fungono da intermediari fra i cittadini e i servizi dello Stato: il portale trasferisce le richieste dei cittadini e conserva i documenti della pubblica amministrazione fino a quando il cittadino non li richiama.

Ogni servizio della pubblica amministrazione rimane responsabile del trattamento di dati effettuato per finalità proprie. Tuttavia, anche il portale stesso può essere considerato un responsabile del trattamento. Esso in effetti tratta (cioè raccoglie e trasferisce al servizio competente) le richieste dei cittadini e i documenti pubblici (li conserva e ne regola l'accesso, ad es. le possibilità di fare il download) per finalità diverse (prestazione di servizi di amministrazione elettronica) da quelle per cui i dati sono inizialmente trattati dai singoli servizi della pubblica amministrazione. Questi responsabili del trattamento, fra gli altri obblighi, devono garantire la sicurezza del sistema di trasferimento dei dati personali dall'utente alla pubblica amministrazione, poiché a livello macroscopico questo trasferimento è una parte fondamentale dell'insieme dei trattamenti effettuati attraverso il portale.

Un'altra struttura possibile è l'"approccio basato sull'origine", che si configura quando ogni responsabile del trattamento risponde dei dati che introduce nel sistema. È il caso di alcune banche dati a livello europeo, nell'ambito delle quali la responsabilità - e quindi l'obbligo di intervenire in caso di richieste di accesso e rettifica - è attribuita in base all'origine nazionale dei dati personali.

Un altro interessante scenario è quello dei social network su Internet.

Esempio n. 12: Social network

I fornitori di servizi di social network propongono piattaforme di comunicazione on-line che consentono di pubblicare e scambiare informazioni fra utenti. Questi fornitori di servizi sono i responsabili del trattamento dei dati, poiché determinano sia le finalità che gli strumenti dell'elaborazione di tali informazioni. Gli utenti di questi network, caricando dati personali anche di terzi, potrebbero essere considerati responsabili del trattamento nella misura in cui le loro attività non rientrino nell'"esenzione domestica" [17].

Dopo aver analizzato i casi in cui i vari soggetti determinano insieme solo parte delle finalità e degli strumenti, presentiamo in appresso una situazione molto chiara e definita, cioè quella in cui più soggetti determinano insieme tutte le finalità e tutti gli strumenti delle attività di trattamento, dando luogo a una corresponsabilità a pieno titolo.

In quest'ultimo caso è facile stabilire chi è competente e nella posizione di garantire i diritti degli interessati e di adempiere agli obblighi relativi alla protezione dei dati. Tuttavia, nei casi in cui i vari corresponsabili condividono finalità e strumenti in modo asimmetrico, stabilire quale responsabile del trattamento è competente - e deve rispondere - per quali diritti ed obblighi degli interessati è molto più complesso.

Necessità di chiarire la distribuzione delle responsabilità

In primo luogo va sottolineato, specialmente nei casi di corresponsabilità, che il fatto di non potere adempiere direttamente a tutti gli obblighi incombenti a un responsabile del trattamento (garantire l'informazione, il diritto d'accesso, ecc.) non esclude tale qualifica: nella pratica può accadere di fatto che a tali obblighi possano facilmente adempiere, per conto del responsabile del trattamento, altre parti talvolta più vicine all'interessato. Ciò nonostante, il responsabile del trattamento rimane in ogni caso vincolato ai propri obblighi e sarà lui a rispondere di eventuali violazioni.

Secondo un testo presentato dalla Commissione nel corso del processo di adozione della direttiva, il fatto di avere accesso a certi dati personali significherebbe automaticamente essere (co)responsabile del trattamento di tali dati. Questa formulazione non è stata tuttavia mantenuta nel testo finale. L'esperienza mostra inoltre che, da un lato, l'accesso ai dati in quanto tale non fa necessariamente sorgere una responsabilità, e, dall'altro, che il fatto d'aver accesso ai dati non è un prerequisito per essere responsabile del trattamento. Pertanto, nei sistemi complessi in cui intervengono molte figure, l'accesso ai dati personali e gli altri diritti degli interessati possono essere garantiti a diversi livelli da diversi attori.

Per quanto riguarda le conseguenze giuridiche, occorre anche chiedersi se la "corresponsabilità" stabilita dalla direttiva implichi sempre che i responsabili del trattamento rispondano in solido.

L'articolo 23 sulla responsabilità usa il singolare ("il responsabile del trattamento"), lasciando intendere che la risposta è positiva. Tuttavia, come già accennato, nella realtà possono verificarsi vari modi di agire "insieme a", e ciò può portare in alcune circostanze ad una responsabilità solidale, ma non come regola: in molti casi, infatti, i vari responsabili del trattamento possono dover occuparsi - e quindi rispondere - del trattamento di dati personali in fasi diverse e a gradi diversi.

L'essenziale è garantire, anche in contesti complessi di trattamento di dati personali in cui intervengono vari responsabili, l'osservanza delle norme sulla protezione dei dati e una chiara attribuzione delle responsabilità per possibili violazioni di tali norme. Questo per evitare che venga meno la protezione dei dati personali o che si producano un "conflitto negativo di competenze" o delle falle, in una situazione in cui nessuna delle parti si assumerebbe gli obblighi o assicurerebbe i diritti derivanti dalla direttiva.

In queste eventualità, più che mai, è importante fornire agli interessati informazioni chiare, che specifichino le varie fasi e i vari attori del trattamento. Sarebbe inoltre opportuno chiarire se ogni responsabile del trattamento è competente a garantire tutti i diritti degli interessati, oppure indicare quale responsabile è competente per quale diritto.

Esempio n. 13: Banche e centri di informazioni sui clienti morosi

Varie banche possono creare - se la legge lo consente - un "centro di informazioni" comune, in cui ognuna di esse immette informazioni (dati) sui clienti morosi e a cui ognuna di esse ha totale accesso. Alcune legislazioni prevedono che tutte le richieste degli interessati, ad es. per l'accesso ai dati o per la loro cancellazione, siano presentate a un solo "punto di ingresso", cioè il provider. Ad esso spetta trovare un appropriato responsabile del trattamento e fare in modo che l'interessato riceva risposte pertinenti. L'identità del provider è pubblicata nel registro del trattamento dei dati. Altri ordinamenti nazionali prevedono che tali centri di informazioni siano gestiti da persone giuridiche distinte in qualità di responsabili del trattamento, mentre le richieste di accesso degli interessati sono gestite dalle banche partecipanti in qualità di intermediari.

Esempio n. 14: Pubblicità comportamentale

Questa forma di pubblicità utilizza le informazioni raccolte sul comportamento di navigazione degli internauti, ad esempio le pagine visitate o le ricerche effettuate, per selezionare le pubblicità da offrire. Sia gli editori, che molto spesso affittano spazi pubblicitari sui loro siti, che i fornitori di reti pubblicitarie, che riempiono tali spazi con reclame mirate, possono raccogliere e scambiarsi informazioni sugli utenti, in base a specifici accordi contrattuali.

Dal punto di vista della protezione dei dati, l'editore è da considerarsi un responsabile del trattamento autonomo nella misura in cui raccoglie i dati personali dell'utente (profilo utente, indirizzo IP, ubicazione, lingua del sistema operativo, ecc.) per i propri scopi. Il fornitore di reti pubblicitarie sarà a sua volta un responsabile del trattamento nella misura in cui determina le finalità (seguire gli utenti sui vari siti web) o gli strumenti essenziali dell'elaborazione dei dati. A seconda delle condizioni di collaborazione fra l'editore e il fornitore di reti pubblicitarie (ad es. il fatto che l'editore consenta o meno il trasferimento dei dati personali verso il fornitore di reti pubblicitarie, anche ridirigendo l'utente sulla pagine web di quest'ultimo), essi possono essere corresponsabili per l'insieme di trattamenti sottesi alla pubblicità comportamentale.

In tutti i casi i (co)responsabili del trattamento devono assicurare che la complessità e le peculiarità tecniche del sistema di pubblicità comportamentale non impediscano loro di trovare adeguate modalità di adempimento dei loro obblighi e di garantire i diritti degli interessati. Ciò riguarda in particolare:

- il fatto di informare l'utente che un terzo può avere accesso ai suoi dati. Sarebbe ottimale che a fare ciò fosse l'editore, che è il principale interlocutore dell'utente;
- le condizioni di accesso ai dati personali: il fornitore di reti pubblicitarie dovrebbe rispondere alle domande degli utenti sulle modalità di utilizzo dei loro dati ai fini della pubblicità mirata, e dovrebbe rispettare le richieste di rettifica e di cancellazione dei dati.

Inoltre, gli editori e i fornitori di reti pubblicitarie possono essere soggetti ad altri obblighi derivanti dal diritto civile e dal diritto dei consumatori, anche per quanto riguarda la responsabilità civile extracontrattuale e le pratiche commerciali sleali.

Conclusioni preliminari

Le parti che intervengono congiuntamente hanno un certo grado di flessibilità nel distribuire ed attribuire fra di loro obblighi e responsabilità, a condizione che ne garantiscano il pieno rispetto. Le regole su come esercitare responsabilità congiunte dovrebbero in linea di principio essere determinate dai responsabili del trattamento. Tuttavia, anche in questo caso devono essere prese in considerazione le circostanze concrete, per valutare se quanto deciso rispecchia la realtà del trattamento sotteso.

In tale ottica, la valutazione della corresponsabilità dovrebbe tenere conto, da un lato, della necessità di garantire il pieno rispetto delle disposizioni in materia di protezione dei dati e, dall'altro, del fatto che la moltiplicazione dei responsabili del trattamento può anche portare a complicazioni non desiderate e a una possibile mancanza di chiarezza nell'attribuzione delle responsabilità. Ciò rischierebbe di rendere l'intero trattamento illecito, a causa di una mancanza di trasparenza, e di portare a una violazione del principio del trattamento leale.

Esempio n. 15: Piattaforme per la gestione dei dati sanitari

La pubblica autorità di uno Stato membro decide di creare un centro nazionale di scambio di dati sui pazienti fra i prestatori di servizi sanitari. La pluralità di responsabili del trattamento - decine di migliaia - rende la situazione molto poco chiara, al punto da poter compromettere la protezione dei diritti degli interessati (i pazienti). Gli interessati non saprebbero, più, infatti, a chi rivolgersi in caso di reclami, domande e richieste di informazioni, per le rettifiche o l'accesso ai dati personali. Inoltre, l'autorità pubblica è responsabile dell'effettiva concezione del sistema e del modo in cui è utilizzato. Questi elementi portano a concludere che l'amministrazione pubblica che ha creato il centro di scambio debba essere considerata come corresponsabile del trattamento, ma anche come referente per le richieste degli interessati.

In questo contesto, si può affermare che la responsabilità in solido di tutte le parti implicate dovrebbe essere considerata come un modo per eliminare le incertezze, e che quindi andrebbe presa in considerazione solo qualora gli attori interessati non abbiano stabilito un'attribuzione di obblighi e responsabilità chiara ed altrettanto efficace, o qualora tale attribuzione non discenda chiaramente dalle circostanze concrete.

III.2. Definizione di "incaricato del trattamento"

Il concetto di "incaricato del trattamento" non è definito nella Convenzione 108. Il ruolo dell'incaricato del trattamento è riconosciuto per la prima volta dalla prima proposta della Commissione, ma senza l'introduzione del concetto, per "evitare che un trattamento effettuato da un terzo per conto del responsabile abbia come conseguenza una minore protezione della persona interessata". Solo con la proposta modificata della Commissione e in seguito a una proposta del Parlamento europeo, il concetto di "incaricato del trattamento" è stato esplicitamente ed autonomamente enunciato, prima di acquisire l'attuale formulazione nella posizione comune del Consiglio.

Analogamente a quanto avviene per la definizione di "responsabile del trattamento", la definizione di "incaricato del trattamento" prevede, per tale ruolo, una vasta gamma di soggetti ("... persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo ...").

L'esistenza di un incaricato del trattamento dipende da una decisione presa dal responsabile del trattamento. Quest'ultimo può decidere o di trattare i dati all'interno della propria organizzazione - ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità (si veda a contrario l'articolo 2, lettera f))- , o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna, cioè, come indica la relazione della proposta modificata della Commissione,

a una "persona giuridicamente distinta dal responsabile ma che agisce per conto di quest'ultimo".

Per poter agire come incaricato del trattamento occorrono quindi due requisiti: essere una persona giuridica distinta dal responsabile del trattamento ed elaborare i dati personali per conto di quest'ultimo. Questa attività di trattamento può essere limitata a un compito o a un contesto molto specifici o può essere più generale ed ampia.

Inoltre, il ruolo di incaricato del trattamento non deriva dalla natura di un'entità che tratta dei dati, ma dalle sue attività concrete in uno specifico contesto. In altre parole, la stessa entità può intervenire come responsabile per certi trattamenti e come incaricato per altri, e la qualifica di responsabile o incaricato deve essere valutata rispetto a specifici insiemi di dati o di operazioni.

Esempio n. 16: Provider di servizi di hosting su Internet

Un provider di servizi Internet (ISP) che fornisce servizi di hosting è in linea di principio un incaricato del trattamento per i dati personali pubblicati on-line dai suoi clienti, che si rivolgono a lui per l'hosting e la manutenzione del loro sito web. Se tuttavia l'ISP tratta ulteriormente, per scopi propri, i dati contenuti nei siti web, diventa responsabile per tale specifico trattamento. L'analisi sarebbe diversa per un ISP che fornisce servizi di posta elettronica o di accesso a Internet (si veda anche l'esempio n. 1, "Operatori di telecomunicazione").

L'elemento più importante è la condizione secondo cui l'incaricato del trattamento interviene "...per conto del responsabile del trattamento...". Intervenire "per conto di..." significa servire gli interessi di un altro soggetto, e ciò richiama il concetto giuridico di "delega". Nel caso della normativa sulla protezione dei dati, l'incaricato del trattamento deve attuare le istruzioni ricevute dal responsabile del trattamento almeno per quanto attiene alla finalità del trattamento stesso e agli aspetti fondamentali dei mezzi.

In tale ottica, la liceità dell'attività di trattamento dei dati da parte dell'incaricato è determinata dal mandato ricevuto dal responsabile del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, l'incaricato diventa (co)responsabile. La questione della liceità del trattamento sarà valutata alla luce degli altri articoli della direttiva (in particolare gli articoli 6-8). La delega può tuttavia comportare un certo grado di discrezionalità sul modo in cui servire al meglio gli interessi del responsabile del trattamento, consentendo all'incaricato di scegliere gli strumenti tecnici ed organizzativi più adatti.

Esempio n. 17: Esternalizzazione di servizi postali

Degli organismi privati forniscono servizi postali per conto di agenzie (pubbliche) - inviando ad es. assegni familiari e indennità di maternità per conto dell'istituto nazionale di previdenza sociale. In questo caso, un garante per la protezione dei dati personali ha indicato che gli organismi privati in questione dovrebbero essere qualificati come incaricati del trattamento, considerato che il loro compito - benché svolto con un certo grado di autonomia - è limitato solo ad una parte dei trattamenti necessari alle finalità determinate dal responsabile.

Sempre per garantire che esternalizzazione e deleghe non minino il livello di protezione dei dati, la direttiva contiene due disposizioni specificamente rivolte all'incaricato del trattamento e che definiscono in modo molto dettagliato i suoi obblighi in materia di riservatezza e sicurezza.

- L'articolo 16 stabilisce che lo stesso incaricato del trattamento, così come chiunque agisca sotto la sua autorità, non deve elaborare i dati personali ai quali ha accesso se non dietro istruzione del responsabile del trattamento.

- L'articolo 17, in relazione alla sicurezza dei trattamenti, stabilisce la necessità di un contratto o di un atto giuridico vincolante che disciplini le relazioni fra il responsabile e l'incaricato del trattamento. Deve trattarsi, a fini di conservazione delle prove, di un contratto stipulato per iscritto che deve avere un contenuto minimo, e che deve prevedere segnatamente che l'incaricato del trattamento dei dati

operi soltanto su istruzioni del responsabile del trattamento, e che attui misure tecniche e organizzative per proteggere adeguatamente i dati personali. Il contratto deve includere una descrizione sufficientemente dettagliata del mandato dell'incaricato del trattamento.

A tale riguardo va osservato che in molti casi i fornitori di servizi specializzati in certe operazioni di trattamento (ad esempio pagamento di stipendi) stabiliscono servizi e contratti standard da far firmare ai responsabili del trattamento, fissando di fatto una certa modalità-tipo di trattamento dei dati personali [18]. Tuttavia, il fatto che il contratto e le sue dettagliate condizioni generali siano preparate dal fornitore di servizi invece che dal responsabile del trattamento non basta in sé per concludere che il fornitore di servizi debba essere considerato come un responsabile del trattamento, nella misura in cui quest'ultimo ha liberamente accettato le clausole contrattuali e di conseguenza la piena responsabilità a riguardo.

Nello stesso spirito, lo squilibrio fra il potere contrattuale di un piccolo responsabile del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati.

Esempio n. 18: Piattaforme di posta elettronica

John Smith cerca una piattaforma di posta elettronica per sé e per i cinque dipendenti della sua impresa. Ne trova una adatta e di facile utilizzo - nonché l'unica gratuita -, ma scopre che conserva i dati personali per un lasso di tempo eccessivo e li trasferisce a paesi terzi senza adeguate garanzie. Le condizioni contrattuali sono, per di più, "prendere o lasciare".

In questa situazione il sig. Smith deve cercare un altro provider, oppure - in caso di presunta inosservanza delle norme sulla protezione dei dati o in mancanza, sul mercato, di altri provider adeguati - deve riferire in merito alle autorità competenti, ad esempio il garante per la protezione dei dati, le associazioni di tutela dei consumatori, le autorità antitrust, ecc.

Il fatto che la direttiva richieda un contratto scritto a garanzia della sicurezza del trattamento non significa che, senza un previo contratto, non possano esserci relazioni fra responsabili e incaricati del trattamento. In tale ottica il contratto non è né costitutivo né decisivo, anche se può aiutare a capire meglio le relazioni fra le parti [19]. Pertanto, anche in questo caso va applicato un approccio funzionale, che analizzi gli elementi concreti delle relazioni fra i vari soggetti e il modo in cui sono determinati le finalità e gli strumenti del trattamento. Qualora risulti esistere una relazione responsabile/incaricato del trattamento, queste parti sono obbligate a stipulare un contratto in termini di legge (cfr. articolo 17 della direttiva).

Pluralità di incaricati del trattamento

Succede sempre più spesso che il responsabile del trattamento di dati personali esternalizzi le operazioni affidandole a più incaricati del trattamento. Questi possono avere una relazione diretta col responsabile del trattamento oppure possono essere subcontraenti cui gli incaricati hanno delegato parte delle attività di trattamento a loro affidate.

Le nuove tecnologie rendono queste strutture complesse (multilivello o estese) sempre più frequenti, e alcune legislazioni nazionali vi fanno esplicitamente riferimento. Nulla, nella direttiva, impedisce che, per motivi organizzativi, più entità possano essere designate come incaricati o subcontraenti, anche suddividendo i compiti rilevanti. Nel procedere all'elaborazione dei dati tutti questi soggetti, però, devono attenersi alle istruzioni date dal responsabile del trattamento.

Esempio n. 19: Griglie informatiche

Le grandi infrastrutture di ricerca usano sempre di più strutture informatiche distribuite, specialmente griglie, per sfruttare una maggiore capacità di calcolo e di conservazione dei dati. Le griglie sono installate in diverse infrastrutture di ricerca stabilite in diversi paesi. Una griglia europea può, ad esempio, essere composta da griglie nazionali, che a loro volta sono sotto la responsabilità di un organismo nazionale. La griglia europea, però, può anche non avere alcun organismo centrale che sia responsabile del suo funzionamento. I ricercatori che usano una griglia di questo tipo generalmente non possono individuare dove avviene esattamente il trattamento dei loro dati, e quindi chi è l'incaricato responsabile (la situazione è ancora più complicata se ci sono infrastrutture di griglia in paesi terzi). Se un'infrastruttura di griglia usa i dati in modo non autorizzato, essa può essere considerata responsabile del trattamento, se non agisce per conto dei ricercatori.

La questione strategica in questo caso è che - vista la pluralità di soggetti che intervengono nel processo - gli obblighi e le responsabilità derivanti dalla legislazione sulla protezione dei dati devono essere chiaramente attribuiti e non si devono disperdere lungo la catena di esternalizzazione e di subcontraenti. In altre parole, va evitata una catena di (sotto)incaricati che minerebbe o addirittura impedirebbe un effettivo controllo e chiare responsabilità per le attività di trattamento - a meno che le responsabilità delle varie parti non siano chiaramente stabilite.

In tale ottica, sulla scia di quanto descritto al paragrafo III.1.b, anche se non è necessario che il responsabile del trattamento definisca e concordi tutti i dettagli quanto ai mezzi messi in atto per perseguire le finalità previste, è comunque necessario che questi sia almeno informato dei principali elementi della struttura del trattamento (ad esempio i soggetti implicati, le misure di sicurezza, le garanzie per il trattamento in paesi terzi, ecc.), in modo da essere sempre in grado di controllare i dati trattati per suo conto.

Va anche considerato che, se la direttiva designa il responsabile del trattamento quale soggetto che risponde delle attività svolte, essa non impedisce comunque che le legislazioni nazionali sulla protezione dei dati prevedano anche, in certi casi, che a rispondere sia l'incaricato del trattamento.

Alcuni criteri possono aiutare a determinare la qualifica dei vari soggetti implicati:

- il livello di istruzioni preliminari date dal responsabile del trattamento dei dati, che definisce il margine di manovra lasciato all'incaricato del trattamento;
- il controllo, da parte del responsabile del trattamento, dell'esecuzione del servizio. Una costante e attenta supervisione del responsabile del trattamento per garantire che l'incaricato si attenga pienamente alle istruzioni e alle condizioni contrattuali indica che il responsabile del trattamento ha il controllo totale ed esclusivo delle operazioni;
- la visibilità/l'immagine data dal responsabile del trattamento agli interessati, e il legittimo affidamento degli interessati sulla base di questa visibilità.

Esempio n. 20: Call-center

Un responsabile del trattamento esternalizza alcune delle sue attività affidandole ad un call-center. Il call-center riceve l'istruzione di chiamare i clienti presentandosi con l'identità del responsabile del trattamento. In questo caso le aspettative dei clienti e il modo in cui il responsabile del trattamento si presenta loro attraverso la società di esternalizzazione portano alla conclusione che questa agisca come incaricato del trattamento per (conto del) responsabile del trattamento.

- Conoscenze specializzate delle parti: in certi casi, il ruolo tradizionale e la competenza professionale del fornitore di servizi svolgono un ruolo predominante che può far scattare la qualifica di responsabile del trattamento.

Esempio n. 21: Avvocati

Un avvocato rappresenta un suo cliente davanti al giudice, e nell'ambito di tale funzione tratta dati personali collegati al caso del cliente. La base legale per poter utilizzare le informazioni necessarie è il mandato dal cliente. Tale mandato, tuttavia, non verte sul trattamento di dati bensì sulla rappresentanza in giudizio, attività per la quale queste professioni hanno tradizionalmente la propria base legale. Tali professioni devono quindi essere considerate come "responsabili del trattamento" indipendenti per quanto riguarda il trattamento dei dati svolto nell'ambito della rappresentanza legale del cliente.

In un contesto diverso, può a sua volta risultare determinante una valutazione più approfondita dei mezzi posti in atto per raggiungere le finalità perseguite.

Esempio n. 22: Sito web "Oggetti smarriti"

Un sito web "Oggetti smarriti" è stato presentato come un mero incaricato del trattamento: a determinare il contenuto e quindi, a livello microscopico, la finalità (ad es. ritrovare una spilla perduta, un pappagallo, ecc.), sarebbero infatti le persone che pubblicano gli annunci. Un garante per la protezione dei dati ha respinto questa argomentazione. Il sito web è stato creato allo scopo commerciale di trarre profitto dalla pubblicazione degli annunci; il fatto che non determini quali oggetti specifici possono essere oggetto degli annunci (ma solo le categorie di oggetti) non è fondamentale, visto che la definizione di "responsabile del trattamento dei dati" non include espressamente la determinazione di un contenuto. Il sito web determina le condizioni di pubblicazione degli annunci ed è responsabile della correttezza del contenuto.

Vi è stata in passato una tendenza a far coincidere in generale l'esternalizzazione con la funzione dell'incaricato del trattamento. Oggi le situazioni e le valutazioni sono spesso molto più complesse.

Esempio n. 23: Contabili

La qualifica del contabile può variare a seconda del contesto. Quando fornisce servizi ai cittadini e ai piccoli imprenditori sulla base di istruzioni molto generali ("Mi prepari la dichiarazione dei redditi"), il contabile - come gli avvocati, che agiscono in condizioni analoghe e per ragioni comparabili - sarà un responsabile del trattamento. Tuttavia, se lavora per una società, ed è vincolato alle dettagliate istruzioni del contabile interno, per effettuare, ad esempio un audit dettagliato, sarà, se non un dipendente, un incaricato del trattamento, dato che le istruzioni saranno molto chiare e il suo potere discrezionale di conseguenza limitato. Interviene tuttavia una riserva molto importante: quando ritiene di avere scoperto un'irregolarità che è obbligato a segnalare, allora, in virtù degli obblighi professionali cui è tenuto, agisce in modo indipendente in qualità di responsabile del trattamento.

A volte, la complessità dei trattamenti può portare a mettere maggiormente l'accento sul margine di manovra di coloro cui è stato affidato il trattamento dei dati personali, ad esempio quando comporta uno specifico rischio per la privacy. Introdurre nuovi strumenti per il trattamento può favorire la qualifica di responsabile piuttosto che quella di incaricato del trattamento. In questi casi si può anche arrivare a un chiarimento - e a una designazione del responsabile del trattamento - come esplicitamente previsto dalla legge.

Esempio n. 24: Trattamento per scopi storici, scientifici e statistici

Il diritto nazionale può introdurre, per quanto riguarda il trattamento di dati personali per scopi storici, scientifici e statistici, il concetto di organismo intermediario, designante l'organismo incaricato di trasformare dati non codificati in dati codificati, in modo che il responsabile del trattamento per scopi storici, scientifici e statistici non sia in grado di identificare gli interessati.

Se più responsabili di operazioni di trattamento iniziali trasmettono dati a uno o più terzi per un trattamento ulteriore a scopi storici, scientifici e statistici, i dati sono prima codificati dall'organismo intermedio. In questo caso tale organismo intermedio può essere considerato come responsabile del trattamento in applicazione di specifiche norme nazionali, e sarà soggetto a tutti gli obblighi derivanti (pertinenza dei dati, informazione dell'interessato, notificazione, ecc.). Quando si riuniscono i dati provenienti da diverse fonti, la loro protezione è particolarmente minacciata, cosa che giustifica la responsabilità propria dell'organismo intermedio. Di conseguenza, esso non è semplicemente ritenuto un incaricato del trattamento ma è pienamente considerato come responsabile del trattamento in virtù del diritto nazionale.

Analogamente, importante è anche il potere di decisione autonomo lasciato alle varie parti che intervengono nel trattamento. L'esempio dei test clinici per i medicinali mostra che la relazione fra i finanziatori e le entità esterne incaricate di effettuare i test dipende dal margine di manovra lasciato a queste ultime rispetto al trattamento dei dati. Ciò implica che ci possa essere più di un responsabile del trattamento, ma anche più di un incaricato o persona cui è stato affidato il trattamento.

Esempio n. 25: Test clinici sui medicinali

La società farmaceutica XYZ finanzia alcuni test di medicinali e seleziona i centri di sperimentazione candidati valutandone l'ammissibilità e gli interessi; elabora il protocollo del test, fornisce le necessarie indicazioni ai centri per quanto riguarda il trattamento dei dati e verifica che i centri osservino sia il protocollo che le rispettive procedure interne.

Benché il finanziatore non raccolga direttamente alcun dato, acquisisce i dati dei pazienti raccolti dai centri di sperimentazione e li tratta in vari modi (valutando le informazioni contenute nei documenti medici; ricevendo i dati relativi agli effetti collaterali; inserendo tali dati nella banca dati pertinente; effettuando analisi statistiche per arrivare ai risultati dei test). Il centro di sperimentazione effettua il test autonomamente, ma sempre conformemente alle indicazioni del finanziatore; fornisce le note informative ai pazienti e ottiene il loro consenso quanto al trattamento dei dati che li riguardano; autorizza i collaboratori del finanziatore ad accedere ai documenti medici originali dei pazienti nell'ambito di attività di monitoraggio; gestisce tali documenti ed è responsabile della loro conservazione. Risulta quindi che le responsabilità siano affidate ai singoli attori.

In questo contesto, sia i centri di sperimentazione che i finanziatori prendono decisioni importanti quanto alle modalità di trattamento dei dati personali relativi ai test clinici. Di conseguenza, possono essere considerati corresponsabili del trattamento. La relazione fra il finanziatore e i centri di sperimentazione potrebbe essere interpretata in modo diverso nei casi in cui il finanziatore determini le finalità e gli aspetti fondamentali dei mezzi, lasciando invece al ricercatore uno strettissimo margine di manovra.

III.3. Definizione di "terzi"

Il concetto di "terzi" non era definito dalla Convenzione 108, ma è stato introdotto dalla proposta modificata della Commissione in seguito a un emendamento proposto dal Parlamento europeo. Secondo la relazione, l'emendamento è stato riformulato per precisare che i terzi non includono l'interessato, il responsabile del trattamento e le persone autorizzate all'elaborazione dei dati sotto l'autorità diretta del responsabile del trattamento o per suo conto, come avviene con l'incaricato del trattamento. Ciò significa che "le persone che lavorano in un'altra impresa anche se quest'ultima fa parte di uno stesso gruppo o holding dovrebbero in linea di massima essere considerate come terzi", mentre, per contro, "le succursali di una banca che eseguono trattamenti relativi alla gestione della clientela posta sotto l'autorità diretta della sede non dovrebbero essere considerati come terzi".

La direttiva usa il termine "terzi" in modo non tanto diverso da quello in cui tale concetto è generalmente utilizzato nel diritto civile, secondo cui il terzo è di solito un soggetto che non è parte di un'entità o di un accordo. Nel contesto della protezione dei dati, tale concetto dovrebbe essere interpretato come riferimento a qualsiasi soggetto che non sia specificamente legittimato o autorizzato - in base, ad esempio, al suo ruolo di responsabile del trattamento, incaricato del trattamento o loro dipendente - a trattare dati personali.

La direttiva utilizza questo concetto in molte disposizioni, generalmente per stabilire divieti, limitazioni e obblighi nell'eventualità in cui certi dati personali possano essere elaborati da parti che originariamente non avrebbero dovuto farlo.

In questo contesto, si può concludere che un terzo che riceva dati personali - lecitamente o meno - sarebbe in linea di principio un nuovo responsabile del trattamento, purché ricorrano le altre condizioni relative all'attribuzione di tale qualifica e sia applicata la legislazione in materia di protezione dei dati.

Esempio n. 26: Accesso non autorizzato da parte di un dipendente

Un dipendente di una società, nell'esercizio delle sue funzioni, viene a conoscenza di dati personali a cui non ha diritto di accedere. In questo caso, il dipendente va considerato come un "terzo" rispetto al suo datore di lavoro, con tutte le relative conseguenze e le responsabilità in termini di liceità della comunicazione e di trattamento dei dati.

[10] Relativo al trasferimento alle autorità americane, ai fini della lotta contro il finanziamento del terrorismo, di dati bancari raccolti dalla SWIFT per realizzare operazioni finanziarie per conto di banche e istituti finanziari.

[11] Si veda, *infra*, l'interferenza con concetti esistenti in altri settori del diritto (ad es. quello di "titolare del diritto" per la proprietà intellettuale o la ricerca scientifica, o quello di "responsabilità" in diritto civile).

[12] Un'autorità per la protezione dei dati ha esaminato la questione del controllo in un reclamo presentato da un interessato contro il ricevimento di pubblicità indesiderata per e-mail. Col reclamo l'interessato chiedeva al provider della rete di comunicazione di confermare o negare di essere il mittente dei messaggi pubblicitari elettronici. L'autorità per la protezione dei dati ha concluso che una società che si limita a fornire al cliente l'accesso a un rete di comunicazione - e che non procede ad alcuna trasmissione di dati, non seleziona i destinatari né modifica le informazioni contenute nei messaggi -, non può essere considerata come responsabile del trattamento dei dati.

[13] Si applica un ragionamento analogo per quanto riguarda il [regolamento \(CE\) n. 45/2001](#), il cui articolo 2, lettera d) si riferisce all'"istituzione o l'organismo della Comunità, la direzione generale, l'unità o qualunque altra entità organizzativa". La prassi in materia di controllo ha chiaramente stabilito che tutti i funzionari delle istituzioni e degli organismi dell'UE che sono stati designati "responsabili del trattamento", agiscono per conto dell'organismo per cui lavorano.

[14] Cfr. il testo "Comparative Study on the Situation in the 27 Member States as regards the Law Applicable to Non-contractual Obligations Arising out of Violations of Privacy and Rights relating to Personality" ("Studio comparativo sulla situazione dei 27 Stati membri per quanto riguarda il diritto applicabile alle obbligazioni non contrattuali derivanti dalla violazione della privacy e dei diritti relativi alla personalità"), febbraio 2009, consultabile al seguente indirizzo: http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

[15] Ciò non esclude che i diritti nazionali possano prevedere una responsabilità penale o amministrativa non solo per il responsabile del trattamento, ma per qualsiasi persona che violi le norme sulla protezione dei dati.

[16] Cfr. ad es. la [direttiva 2008/99/CE](#), del 19 novembre 2008, sulla tutela penale dell'ambiente, e la decisione quadro del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo. Gli strumenti giuridici sono basati sull'articolo 29, sull'articolo 31, lettera e) e sull'articolo 34, paragrafo 2, lettera b) del TUE, oppure corrispondono alle basi giuridiche degli strumenti usati nel primo pilastro, derivanti dalla giurisprudenza della Corte nelle cause C-176/03, Commissione/Consiglio, Racc. 2005, pag. I-7879 e C-440/05, Commissione/Consiglio, Racc. 2007, pag. I-9097. Cfr. anche la comunicazione della

Commissione (2005) 583 def.

[17] Per maggiori dettagli ed esempi cfr. il parere 5/2009 del Gruppo di lavoro Articolo 29 sui social network on-line, adottato il 12 giugno 2009 (WP 163).

[18] L'elaborazione delle clausole contrattuali da parte del fornitore di servizi lascia impregiudicato il fatto che gli elementi fondamentali del trattamento, quali esposti al paragrafo III.1.b, sono determinati dal responsabile del trattamento.

[19] In alcuni casi, tuttavia, l'esistenza di un contratto scritto può costituire una condizione necessaria per essere automaticamente qualificato come incaricato del trattamento in certi contesti. In Spagna, ad esempio, la relazione sui call-center definisce come incaricati del trattamento tutti i call-center nei paesi terzi, purché rispettino il contratto. Questo vale anche se il contratto è stato redatto dall'incaricato del trattamento e il responsabile semplicemente vi "aderisce".

IV. Conclusioni

Il concetto di "responsabile del trattamento" dei dati, e la sua interazione col concetto di "incaricato del trattamento", svolgono un ruolo cruciale nell'applicazione della [direttiva 95/46/CE](#), poiché determinano chi risponde dell'osservanza delle norme relative alla protezione dei dati, il modo in cui gli interessati possono esercitare i loro diritti, il diritto nazionale applicabile e l'efficacia del lavoro delle autorità per la protezione dei dati.

La differenziazione organizzativa nel settore pubblico e privato, lo sviluppo delle TIC e la dimensione mondiale del trattamento dei dati aumentano la complessità di tale trattamento e rendono necessario un chiarimento dei concetti sopra indicati, per garantirne un'efficace applicazione e osservanza nella pratica.

Il concetto di responsabile del trattamento è autonomo - va interpretato cioè principalmente alla luce delle disposizioni comunitarie relative alla protezione dei dati -, e funzionale, nel senso che è finalizzato all'assegnazione di responsabilità laddove intervenga un'influenza effettiva: si basa quindi su un'analisi fattuale piuttosto che formale.

La definizione della direttiva si articola intorno a tre componenti principali: il soggetto ("la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo"); la possibilità di una responsabilità plurima ("che, da solo o insieme ad altri"), e gli aspetti principali che distinguono il responsabile del trattamento da altre figure ("determina le finalità e gli strumenti del trattamento di dati personali").

L'analisi di queste componenti porta alle seguenti conclusioni principali:

- La capacità di "determinare le finalità e gli strumenti" può derivare da varie circostanze giuridiche e/o concrete: un'esplicita competenza giuridica (quando è la legge a designare il responsabile del trattamento o a conferire il compito o l'obbligo di raccogliere ed elaborare certi dati); disposizioni giuridiche comuni o ruoli tradizionali esistenti che generalmente comportano una certa responsabilità all'interno di certe organizzazioni (ad esempio il datore di lavoro nei confronti dei suoi dipendenti); circostanze concrete ed altri elementi (come relazioni contrattuali, responsabilità effettiva di una parte, visibilità verso gli interessati, ecc.).

Se nessuna di queste categorie di cui sopra è applicabile, la designazione di un responsabile del trattamento dovrà essere considerata "nulla": un organismo che non ha un'influenza, né giuridica né di fatto, per determinare le modalità del trattamento dei dati non può in effetti essere considerato il responsabile del trattamento.

La determinazione della "finalità" del trattamento fa scattare la qualifica di responsabile del trattamento di fatto. Questi può, a sua volta, delegare la determinazione degli "strumenti" del trattamento per quanto riguarda le questioni tecniche od organizzative. Le questioni sostanziali,

attinenti ai fondamenti della liceità del trattamento - dati da trattare, durata della conservazione, accesso, ecc. - devono invece essere determinati dal responsabile del trattamento.

- L'elemento della definizione che si riferisce al soggetto indica una vasta gamma di attori che possono svolgere il ruolo di responsabile del trattamento. Tuttavia, nell'ottica strategica dell'attribuzione delle responsabilità sarebbe preferibile considerare come responsabile del trattamento la società o l'organismo in quanto tali piuttosto che una specifica persona al loro interno. Sono la società o l'organismo a dovere, in ultima analisi, essere considerati responsabili del trattamento dei dati e degli obblighi derivanti dalla normativa sulla protezione dei dati, a meno che non vi siano elementi chiari che indichino che a rispondere di ciò sia una persona fisica - ad esempio nel caso in cui una persona fisica che lavora in una società utilizzi i dati per scopi propri, al di fuori delle attività dell'impresa.

- La possibilità di una responsabilità plurima tiene conto del numero crescente di situazioni in cui varie parti agiscono come responsabili del trattamento. La valutazione di questa corresponsabilità deve essere analoga alla valutazione della responsabilità "singola": occorre adottare un approccio sostanziale e funzionale, che analizzi se le finalità e gli aspetti fondamentali degli strumenti sono determinati da più di una parte.

La partecipazione delle parti alla determinazione delle finalità e dei mezzi del trattamento nel quadro di una corresponsabilità può assumere varie forme e non deve essere necessariamente ripartita in modo uguale. Il presente parere propone numerosi esempi di vari tipi e gradi di corresponsabilità. Gradi diversi di controllo possono dar luogo a gradi diversi di responsabilità e obblighi, e una responsabilità "solidale" non può essere certamente assunta in tutti i casi. Inoltre, è del tutto possibile che in sistemi complessi con molteplici interlocutori, l'accesso ai dati personali e l'esercizio di altri diritti degli interessati possano essere garantiti anche a livelli diversi da diversi attori.

Il presente parere analizza anche il concetto di "incaricato del trattamento", la cui esistenza dipende da una decisione presa dal responsabile del trattamento. Quest'ultimo può decidere o di trattare i dati all'interno della propria organizzazione o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna. Per poter agire come incaricato del trattamento occorrono pertanto due requisiti: da un lato essere una persona giuridica distinta dal responsabile del trattamento, e dall'altro elaborare i dati personali per conto di quest'ultimo. Questa attività di trattamento può essere limitata a un compito o a un contesto molto specifico, oppure può lasciar spazio a un certo margine di discrezionalità sul modo di servire gli interessi del responsabile del trattamento, permettendo all'incaricato del trattamento di scegliere i mezzi tecnici e organizzativi più adeguati.

Inoltre, il ruolo dell'incaricato del trattamento non deriva dalla natura di un soggetto che tratta dati personali, ma dalle sue attività concrete in un contesto specifico e in relazione a specifiche serie di dati od operazioni. Alcuni criteri possono essere utili per determinare la qualifica dei vari attori implicati nel trattamento: il livello di istruzioni preliminari date dal responsabile del trattamento; il controllo, da parte del responsabile del trattamento, del livello del servizio; la visibilità nei confronti degli interessati; la conoscenza specializzata delle parti; il potere di decisione autonoma lasciato alle varie parti.

La categoria restante, quella dei "terzi", indica tutti gli attori che non siano specificamente legittimati né autorizzati - in base, ad esempio, al loro ruolo come responsabili del trattamento, incaricati del trattamento, o loro dipendenti - a trattare dati personali.

Il Gruppo di lavoro riconosce le difficoltà che presenta l'applicazione delle definizioni della direttiva in un contesto complesso, con vari scenari che possono vedere intervenire responsabili e incaricati del trattamento, da soli o congiuntamente con altri, con vari gradi d'autonomia e di responsabilità.

Nella sua analisi, il Gruppo di lavoro sottolinea la necessità di attribuire le responsabilità in modo tale da garantire nella pratica un'adeguata osservanza delle norme sulla protezione dei dati. Ritiene

comunque che non vi sia alcun motivo di pensare che, in tale ottica, l'attuale distinzione fra responsabili del trattamento e incaricati del trattamento possa perdere rilevanza e praticabilità.

Il Gruppo di lavoro spera pertanto che le spiegazioni date nel presente parere, corredate di specifici esempi tratti dall'esperienza quotidiana delle autorità per la protezione dei dati, contribuiranno a fornire effettivi orientamenti sul modo in cui interpretare queste definizioni chiave della direttiva.

Per il Gruppo di lavoro,

Il Presidente

Jacob Kohnstamm