COMMISSIONE EUROPEA

Bruxelles, 25.1.2012
SEC(2012) 73 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)
e
proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, e la libera circolazione di tali dati

{COM(2012) 11 final}
{SEC(2012) 72 final}

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)
e
proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, e la libera circolazione di tali dati

1. INTRODUZIONE

Da quando è stato adottato l'attuale quadro normativo europeo sulla protezione dei dati nel 1995, le tecnologie e le prassi commerciali sono evolute rapidamente, ponendo nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso; la tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più persone rendono pubblici i loro dati personali a livello mondiale senza essere pienamente consapevoli dei rischi connessi.

Instaurare un clima di fiducia negli ambienti on line è fondamentale per lo sviluppo economico. La mancanza di fiducia frena i consumatori dall'acquistare on line e utilizzare nuovi servizi, compresi quelli offerti on line dalle amministrazioni. Se non vi si porrà rimedio, tale mancanza di fiducia continuerà a rallentare lo sviluppo di applicazioni tecnologiche innovative, ostacolare la crescita economica e impedire al settore pubblico di fruire dei potenziali vantaggi della digitalizzazione dei servizi.

Inoltre, il trattato di Lisbona ha creato, con l'articolo 16 del TFUE, una nuova base giuridica che permette di adottare un approccio modernizzato e globale alla protezione dei dati e alla loro libera circolazione, anche nell'ambito della cooperazione di polizia e giudiziaria in materia penale.

2. DEFINIZIONE DEL PROBLEMA

La valutazione d'impatto presenta e analizza tre grandi problemi.

2.1. Problema 1: ostacoli per le imprese e le autorità pubbliche derivanti dalla frammentazione, dall'incertezza giuridica e dall'applicazione non coerente.

Sebbene la direttiva miri a garantire un livello equivalente di protezione dei dati nell'Unione, tra i vari Stati membri persistono notevoli differenze quanto a norme applicate. Di conseguenza, i responsabili del trattamento possono trovarsi di fronte a 27 legislazioni e

requisiti nazionali diversi all'interno dell'Unione. Ne risulta un quadro normativo frammentato che genera incertezza giuridica e porta a una protezione diseguale delle persone fisiche. Tale situazione produce costi inutili e **oneri amministrativi** per le imprese (pari a **circa 3 miliardi di euro all'anno** nello scenario di base) e disincentiva le imprese, in particolare le PMI, che operano nel mercato unico dall'espandere le loro attività all'estero.

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

2.2. Problema 2: difficoltà per le persone fisiche di mantenere il controllo dei propri dati personali

A causa di questa assenza di armonizzazione delle legislazioni nazionali sulla protezione dei dati e dei poteri diseguali delle autorità di protezione dei dati, l'esercizio dei diritti da parte delle persone fisiche è più difficile in alcuni Stati membri rispetto ad altri, soprattutto in ambito on line.

Il singolo inoltre ha perso il controllo dei propri dati, in quanto il volume di dati scambiati ogni giorno è immenso e spesso l'interessato non è pienamente consapevole del fatto che i suoi dati personali sono raccolti. Sebbene molti europei ritengano che la divulgazione di dati personali faccia sempre più parte della vita moderna[1], il 72% degli internauti europei si inquieta per la grande quantità di dati personali richiesti on line e spesso non sa come esercitare i propri diritti on line.

2.3. Problema 3: lacune e incoerenze nella protezione dei dati personali nel settore della cooperazione di polizia e giudiziaria in materia penale

La direttiva, che si fonda su una base giuridica del mercato interno, esclude specificamente dal suo campo di applicazione la cooperazione di polizia e giudiziaria in materia penale. La decisione quadro adottata nel 2008 per disciplinare il trattamento dei dati nell'ambito della cooperazione di polizia e giudiziaria in materia penale riflette le particolarità della struttura a pilastri dell'Unione prima dell'entrata in vigore del trattato di Lisbona ed è caratterizzata da un **campo di applicazione limitato e da altre varie lacune** che generano incertezza giuridica per le persone fisiche e le autorità di contrasto e difficoltà pratiche in termini di applicazione. Inoltre la decisione quadro prevede numerose possibilità di deroga ai principi generali della protezione dei dati a livello nazionale, e quindi non ne garantisce l'armonizzazione. Tale approccio non solo rischia di privare di contenuto detti principi – e quindi di pregiudicare il diritto fondamentale delle persone fisiche alla protezione dei loro dati personali in questo settore – ma anche di ostacolare il corretto scambio di dati personali tra le autorità nazionali competenti.

3. ANALISI DELLA SUSSIDIARIETÀ E DELLA PROPORZIONALITÀ

Alla luce dei problemi sopra esposti, l'analisi della sussidiarietà indica la necessità di un'azione a livello di Unione per i seguenti motivi:

---

[1] Cfr. Speciale Eurobarometro 359 - *Attitudes on Data Protection and Electronic Identity in the European Union*, giugno 2011, pag. 23.

- il diritto alla protezione dei dati personali è sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. L'articolo 16 del TFUE costituisce la base giuridica per l'adozione di norme dell'Unione sulla protezione dei dati;
- i dati personali possono essere trasferiti attraverso le frontiere nazionali, sia interne che esterne, ad un ritmo sempre crescente. Inoltre, esistono difficoltà pratiche nell'attuare efficacemente la normativa in materia di protezione dei dati e occorre stabilire una cooperazione tra gli Stati membri e le autorità nazionali a livello di Unione, per garantire la coerenza necessaria e un livello elevato di protezione all'interno dell'Unione;
- gli Stati membri non sono in grado da soli di risolvere i problemi posti dalla situazione attuale, in particolare dalla frammentazione delle legislazioni nazionali di attuazione del quadro normativo dell'Unione sulla protezione dei dati;
- sebbene possano adottare politiche per garantire il rispetto di tale diritto, gli Stati membri, in assenza di norme comuni dell'Unione, non riuscirebbero a farlo in modo uniforme e pertanto si creerebbero limitazioni alla circolazione transfrontaliera dei dati personali.

Le **azioni proposte sono proporzionate** in quanto rientrano tra le competenze dell'Unione definite nei trattati e sono necessarie per garantire l'uniformità dell'applicazione della normativa dell'Unione, assicurando una protezione effettiva e uniforme dei diritti fondamentali della persona. L'azione sul piano dell'Unione è essenziale per garantire la credibilità e un livello elevato di protezione dei dati in un mondo globalizzato, consentendo la libera circolazione dei dati. Inoltre, affinché il mercato interno funzioni correttamente è necessario che le disposizioni assicurino condizioni eque agli operatori economici.

4. OBIETTIVI

I tre **obiettivi** principali sono i seguenti:

- **rafforzare la dimensione "mercato interno" della protezione dei dati** riducendo la frammentazione, aumentando la coerenza e **semplificando** il quadro normativo, in modo da eliminare i costi inutili e **diminuire l'onere amministrativo**;
- **rendere più effettivo il diritto fondamentale alla protezione dei dati e consentire alle persone fisiche di mantenere il controllo dei loro dati**;
- **migliorare la coerenza del quadro dell'Unione sulla protezione dei dati**, anche nel settore della cooperazione di polizia e giudiziaria in materia penale, tenendo debito conto dell'entrata in vigore del trattato di Lisbona.

5. OPZIONI STRATEGICHE

5.1. Opzione 1: misure leggere

Quest'opzione prevede principalmente **comunicazioni interpretative della Commissione, strumenti di supporto tecnico e finanziamenti** – oltre alla **promozione della normalizzazione e dell'autoregolazione** – al fine di rafforzare l'applicazione pratica delle norme esistenti da parte dei responsabili del trattamento e aumentare la consapevolezza delle persone. La Commissione proporrà **solo modifiche legislative molto limitate** per chiarire i

concetti esistenti della direttiva e trattare questioni specifiche che non possono essere affrontate efficacemente in altro modo. Tale opzione è pertinente solo per i problemi 1 e 2.

Le modifiche legislative limitate introdurranno espressamente i principi di trasparenza e di minimizzazione dei dati, e una base giuridica per le "norme vincolanti d'impresa" per i trasferimenti internazionali.

5.2. Opzione 2: quadro normativo modernizzato

La Commissione proporrà **modifiche legislative volte ad armonizzare ulteriormente le norme sostanziali**, chiarire disposizioni specifiche ed eliminare le incoerenze derivanti dai diversi approcci adottati dagli Stati membri. Tali proposte offriranno una soluzione ai problemi 1 e 2 poiché permetteranno, da un lato, di **agevolare la circolazione dei dati all'interno dell'Unione e dall'Unione verso i paesi terzi** e, dall'altro, di **chiarire e rafforzare i diritti delle persone fisiche** (ad esempio il diritto di accesso, il "diritto all'oblio", modalità più chiare per manifestare il consenso e notificare le violazioni dei dati) e **aumentare la responsabilità – e il dovere di rendicontazione – dei responsabili del trattamento e degli incaricati del trattamento** (ad esempio introducendo, ove opportuno, l'obbligo di nominare responsabili della protezione dei dati o di effettuare una valutazione d'impatto sulla protezione dei dati). Tale opzione creerà, in particolare, uno **"sportello unico"** per i responsabili del trattamento (ossia un'unica legislazione e un'unica autorità di protezione dei dati competente). Gli requisiti generali di notificazione saranno semplificati ("registrazione di base"). Inoltre le **autorità di protezione dei dati saranno più indipendenti e avranno poteri armonizzati**. La cooperazione e l'assistenza reciproca tra le autorità di protezione dei dati saranno rafforzate, in particolare grazie a un nuovo **"meccanismo di coerenza"** cui parteciperanno sia un "comitato europeo per la protezione dei dati" – di nuova istituzione – sia la Commissione.

Per quanto riguarda la protezione dei dati nel settore della cooperazione di polizia e giudiziaria in materia penale (problema 3), la Commissione presenterà proposte per sostituire la decisione quadro con un **nuovo strumento dal campo di applicazione più ampio** e affronterà le **principali lacune** al fine di rafforzare i diritti delle persone fisiche e facilitare la cooperazione tra autorità di contrasto, tenendo conto delle particolarità del settore delle attività di contrasto.

5.3. Opzione 3: norme giuridiche dettagliate dell'Unione

Tale opzione comprenderà la maggior parte degli elementi dell'opzione 2, l'elaborazione di una **normativa dell'Unione molto più dettagliata**, anche di tipo settoriale (ad esempio in campo medico e sanitario), e una **struttura centralizzata a livello di Unione per il controllo dell'applicazione** (creazione di un'autorità europea di protezione dei dati). Implicherà inoltre l'eliminazione dei requisiti generali di notificazione (eccezion fatta per il controllo preliminare dei trattamenti rischiosi), la creazione di un regime di certificazione valido in tutta l'Unione per procedimenti e prodotti "ottemperanti ai principi di protezione" e la definizione di sanzioni penali armonizzate in tutta l'Unione per le violazioni delle norme sulla protezione dei dati. Il consenso costituirà il "motivo principale" per il trattamento dei dati.

Per quanto riguarda la cooperazione di polizia e giudiziaria in materia penale, oltre alle misure sostanziali di cui all'opzione 2, saranno introdotte norme dettagliate sul diritto di accesso delle persone (sempre diretto). Saranno inoltre **modificate le disposizioni pertinenti di tutti**

gli strumenti vigenti dell'ex terzo pilastro in modo da allinearli pienamente alle nuove norme armonizzate ed estese.

6. VALUTAZIONE DEGLI IMPATTI

6.1. Opzione 1: misure leggere

Le comunicazioni interpretative della Commissione sulle disposizioni della direttiva non saranno vincolanti, pertanto il loro **impatto sulla riduzione dell'incertezza giuridica e dei costi sarà limitato**. Una maggiore autoregolamentazione a livello di Unione contribuirà ad aumentare la chiarezza per i responsabili del trattamento in settori specifici, ma, senza un quadro normativo di fondo dell'Unione chiaro e armonizzato, **non sarà sufficiente** per garantire un'applicazione effettiva e coerente delle norme.

Le campagne di sensibilizzazione aiuteranno le persone a diventare più consapevoli dei propri diritti in materia di protezione dei dati e delle relative modalità pratiche di esercizio. **Saranno tuttavia insufficienti** a far conoscere i diritti nei casi in cui questi non sono chiaramente definiti dalla legge. **I chiarimenti legislativi** sui principi di trasparenza, minimizzazione dei dati e adeguatezza e sulle norme vincolanti d'impresa aumenteranno l'armonizzazione e la certezza giuridica per i singoli e le imprese.

Per quanto riguarda il controllo dell'applicazione della legge, le comunicazioni della Commissione non basteranno per superare le resistenze degli Stati membri a modificare le norme nazionali per conferire maggior indipendenza e poteri armonizzati alle autorità di protezione dei dati. Un maggior coordinamento da parte del gruppo di lavoro "articolo 29" e scambi più intensi tra le autorità di protezione dei dati avranno un impatto positivo ai fini dell'applicazione più coerente delle norme; tuttavia, **le persistenti divergenze tra le legislazioni nazionali e la loro interpretazione limiteranno l'effetto di un miglioramento della cooperazione tra le autorità di protezione dei dati**.

L'**impatto economico e finanziario atteso da tale opzione è limitato** e i problemi individuati non saranno risolti.

6.2. Opzione 2: quadro normativo modernizzato

L'incertezza giuridica per le imprese private e le autorità pubbliche **sarà notevolmente ridotta**. Le disposizioni problematiche saranno chiarite e la coerenza aumenterà grazie a un minor margine di interpretazione e alle misure di esecuzione e/o agli atti delegati adottati dalla Commissione.

La sostituzione della notificazione generale delle attività di trattamento con un **sistema di "registrazione" semplificato**, mantenendo i controlli preventivi per i dati sensibili e i trattamenti rischiosi, solleverà i responsabili del trattamento da un obbligo attualmente applicato in modi diversi. Aumentando la responsabilità dei responsabili del trattamento e degli incaricati del trattamento mediante l'introduzione – in determinati casi e con soglie ben definite e mirate – dell'obbligo di nominare responsabili della protezione dei dati e di effettuare una valutazione d'impatto sulla protezione dei dati e introducendo il principio della protezione dei dati fin dalla progettazione si offriranno modalità più agevoli per garantire e dimostrare il rispetto delle norme.

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

L'applicazione della legislazione sarà più coerente grazie al rafforzamento e all'armonizzazione dei poteri delle autorità di protezione dei dati, all'introduzione di un solido meccanismo di cooperazione e assistenza reciproca per i casi che presentano una dimensione europea e all'armonizzazione degli illeciti passibili di sanzioni amministrative.

L'**obbligo di notificare le violazioni dei dati, armonizzato a livello di Unione**, proteggerà meglio le persone, assicurerà la coerenza tra i vari settori ed eviterà gli svantaggi competitivi.

I diritti degli interessati e il controllo di ciascuno dei propri dati saranno significativamente rafforzati mediante l'introduzione di nuovi diritti e il miglioramento e l'ulteriore chiarificazione di quelli esistenti. I minori formeranno oggetto di apposite misure che terranno conto della loro vulnerabilità. Le associazioni avranno un margine di azione più ampio per sostenere gli interessati nell'esercizio dei loro diritti, incluso in sede giudiziaria.

L'applicazione dei principi generali di protezione dei dati al settore della cooperazione di polizia e giudiziaria in materia penale aumenterà la coerenza globale del quadro UE di protezione dei dati, rispettando nel contempo le specificità proprie delle attività di contrasto. I diritti dei singoli saranno in particolare rafforzati grazie all'estensione del campo di applicazione delle norme di protezione dei dati in questo settore ai trattamenti "nazionali", alla definizione di condizioni che garantiscano il diritto di accesso e all'introduzione di norme più rigorose sulla limitazione delle finalità.

In termini di **impatto economico e finanziario**, l'obbligo per gli operatori economici di grandi dimensioni (con più di 250 dipendenti) di designare un responsabile della protezione dei dati **non genererà costi sproporzionati**, in quanto tale figura è già comune in tali imprese. I costi di conformità dovrebbero ammontare a 320 milioni di euro all'anno. Tale obbligo si applicherà a una fascia minima necessaria di responsabili del trattamento, dato che di norma le PMI ne saranno escluse, tranne quando le loro attività di trattamento dei dati comportano rischi significativi per la protezione dei dati. Le autorità pubbliche e gli organismi pubblici saranno autorizzati a nominare un unico responsabile della protezione dei dati per più entità (ad esempio per più succursali, dipartimenti, uffici), tenuto conto della loro struttura organizzativa.

La semplificazione delle norme sui trasferimenti internazionali (ad esempio grazie all'estensione della portata delle "norme vincolanti d'impresa") avrà un impatto positivo anche sulla competitività delle imprese europee a livello internazionale.

Il rafforzamento dell'indipendenza e dei poteri delle autorità di protezione dei dati e l'obbligo per gli Stati membri di fornire loro risorse sufficienti implicheranno costi supplementari per quelle autorità pubbliche che attualmente non dispongono di poteri appropriati e risorse adeguate.

Il nuovo meccanismo di cooperazione e assistenza reciproca tra le autorità di protezione dei dati comporterà costi supplementari anche per le autorità nazionali di protezione dei dati e il garante europeo della protezione dei dati. Ad esempio gli incarichi supplementari del garante

connessi all'espletamento delle funzioni di segreteria del comitato europeo per la protezione dei dati – che sostituirà il gruppo di lavoro "articolo 29" – e, in particolare, la partecipazione al meccanismo di coerenza renderanno necessario aumentare il suo attuale bilancio in media di 3 milioni di euro all'anno per i primi sei anni, inclusi i costi per l'assunzione di altre 10 persone.

6.3. Opzione 3: norme giuridiche dettagliate dell'Unione

Grazie all'introduzione di disposizioni giuridiche più dettagliate, anche di tipo settoriale, che vanno oltre alle misure previste dall'opzione 2, **si ridurranno al massimo le disparità tra Stati membri**. Tuttavia questi potranno non avere margine di flessibilità sufficiente per tener conto delle specificità nazionali.

La soppressione totale delle notificazioni – tranne per i controlli preventivi – semplificherà enormemente il quadro normativo e ridurrà l'onere amministrativo.

L'istituzione di un'agenzia europea per la protezione dei dati migliorerà sensibilmente la **coerenza dell'applicazione della legislazione** ed eliminerà le incoerenze nei casi a chiara dimensione europea, ma i poteri di una tale agenzia potrebbero andare troppo lontano rispetto al diritto dell'Unione. Quest'opzione sarà estremamente costosa per il bilancio dell'Unione. Le sanzioni penali armonizzate rafforzeranno la coerenza dell'applicazione della legislazione, tuttavia è molto probabile che gli Stati membri si opporranno fermamente a sanzioni di questo tipo.

I diritti degli interessati, compresi i diritti dei minori, saranno ulteriormente rafforzati, ad esempio estendendo la definizione di dati sensibili in modo che includa anche i dati relativi ai minori, i dati biometrici e i dati finanziari. L'introduzione di un diritto di azione collettiva potrà permettere di massimizzare i diritti attraverso l'azione legale. I diritti dei singoli dovrebbero risultare ulteriormente rafforzati dall'armonizzazione del livello di sanzioni, incluse quelle penali, a livello di Unione.

Le modifiche esplicite di tutti gli strumenti al fine di estendere le norme generali sulla protezione dei dati al settore della cooperazione di polizia e giudiziaria in materia penale avranno un impatto positivo in termini di coerenza delle norme in questo settore e di rafforzamento dei diritti dei singoli. Tuttavia un approccio così radicale incontrerà le resistenze degli Stati membri e sarà politicamente difficile da realizzare.

7. CONFRONTO DELLE OPZIONI

L'***opzione 1*** comporterà un livello di costi di conformità e amministrativi basso, soprattutto per i responsabili del trattamento privati, in quanto la maggior parte dei costi supplementari sarà a carico delle autorità pubbliche nazionali e dell'Unione. Parallelamente avrà un **impatto positivo limitato sui problemi individuati e sulla realizzazione degli obiettivi strategici**.

Sotto il profilo della fattibilità politica, sebbene le proposte non siano controverse, questa opzione incontrerebbe le resistenze delle parti interessate, in quanto la sua portata e la sua incidenza sui problemi sono limitate, e non sarebbe considerata abbastanza ambiziosa.

L'*opzione 2* diminuirà significativamente la frammentazione e l'incertezza giuridica. Dovrebbe contribuire in una misura molto più larga alla risoluzione dei problemi individuati e alla realizzazione degli obiettivi strategici. Il bilanciamento dei **costi di adeguamento e**

amministrativi associati a tale opzione dovrebbe essere ragionevole, considerati i conseguenti vantaggi e risparmi pari a circa 2,3 miliardi di euro all'anno in termini di onere amministrativo – aspetto particolarmente importante per le imprese. Tale opzione garantirà un'applicazione globale migliore e più coerente. La soppressione delle notificazioni e il passaggio a un sistema più semplice di "registrazione di base" semplificheranno il quadro normativo e ridurranno l'onere amministrativo.

Quanto alla sua accettazione da parte delle parti interessate, tale opzione nel complesso sarà accolta favorevolmente dagli operatori economici e dalle autorità pubbliche, in quanto ridurrà globalmente i loro costi di conformità, in particolare quelli connessi all'attuale regime frammentato. I soggetti attivi nella protezione dei dati, in particolare le autorità di protezione dei dati, si compiaceranno del rafforzamento dei diritti in tale settore. Per quanto riguarda il terzo obiettivo generale, tale opzione contribuirà alla realizzazione degli obiettivi miranti a garantire una **maggiore coerenza delle norme sulla protezione dei dati nel settore della cooperazione di polizia e giudiziaria in materia penale**, abrogando e conformando al trattato di Lisbona la decisione quadro, in modo da colmarne le lacune, in particolare estendendone il campo di applicazione ai trattamenti "nazionali".

L'***opzione 3*** comprende la maggior parte delle misure previste dall'opzione 2, ma si spinge molto più lontano sotto diversi aspetti. Avrà quindi un **impatto positivo elevato in termini sia di riduzione dei costi connessi alla frammentazione giuridica sia di rafforzamento dei diritti delle persone fisiche**. Inoltre permetterà di massimizzare la coerenza delle norme di protezione dei dati dell'ex terzo pilastro e di aumentare gli standard di protezione dei dati in tale contesto. Tuttavia, alcune misure previste da tale opzione comporteranno **costi di conformità eccessivi o potranno scontrarsi con una forte opposizione delle parti interessate**. Per giunta, la modifica simultanea di tutti gli strumenti dell'ex terzo pilastro sarà particolarmente complessa e controversa sotto il profilo politico.

Opzione prescelta:

L'***opzione prescelta*** è l'opzione 2 in combinazione con:

– la soppressione degli obblighi di notificazione prevista dall'opzione 3, e

– alcune misure leggere previste dall'opzione 1: l'incentivazione di tecnologie che rafforzano la protezione della vita privata e di regimi di certificazione, e campagne di sensibilizzazione.

L'opzione prescelta è quella che, meglio delle altre, può raggiungere gli obiettivi senza comportare costi di conformità eccessivi e permettendo una riduzione dell'onere amministrativo.

Il rafforzamento delle norme di protezione dei dati dovrebbe generare alcuni costi di conformità supplementari, in particolare per i responsabili del trattamento che effettuano attività di trattamento rischiose. Tuttavia, un solido regime di protezione dei dati può offrire un vantaggio competitivo per l'economia dell'Unione, in quanto il livello più elevato di protezione e l'attesa riduzione del numero di violazioni dei dati personali possono aumentare la fiducia dei consumatori. Obbligare le imprese ad adottare standard elevati di protezione dei dati può anche rivelarsi vantaggioso per le imprese europee nel lungo periodo: esse potrebbero infatti diventare leader mondiali nel settore delle tecnologie di protezione della

privacy o delle soluzioni di protezione della privacy fin dalla progettazione, attirando così imprese e capitali nell'Unione e creando posti di lavoro.

Oltre a ciò, la maggiore armonizzazione renderà il trattamento transfrontaliero dei dati più semplice e meno costoso per le imprese che operano nel mercato interno dell'Unione. Tali imprese saranno quindi incentivate ad espandersi oltre frontiera e ad approfittare dei vantaggi del mercato interno, con effetti positivi tanto per i consumatori quanto per l'economia europea nel suo complesso.

L'opzione prescelta offre inoltre una soluzione equilibrata al problema 3, in quanto rafforza i diritti delle persone fisiche, colma le lacune e riduce le incoerenze per quanto riguarda la protezione dei dati nel settore della cooperazione di polizia e giudiziaria in materia penale, facilitando nel contempo la cooperazione tra autorità di contrasto e rispettando le specificità e le esigenze operative del settore.

8. CONTROLLO E VALUTAZIONE

Il controllo e la valutazione dell'impatto dell'opzione prescelta si concentreranno su elementi quali l'utilizzo dei nuovi strumenti introdotti dalla riforma, i poteri e le risorse delle autorità nazionali di protezione dei dati, le sanzioni per le violazioni della legislazione sulla protezione dei dati, i tempi e i costi impiegati dai responsabili del trattamento per conformarsi alla normativa e lo sviluppo della fiducia delle persone nella protezione dei loro dati personali nell'ambiente on line.