18/IT

WP 254 rev.01

Gruppo di lavoro articolo 29

Criteri di riferimento per l'adeguatezza

Adottati il 28 novembre 2017

Versione emendata e adottata il 6 febbraio 2018

Introduzione

Il Gruppo di lavoro per la protezione dei dati[1] ("Gruppo") ha già presentato un documento di lavoro sui trasferimenti di dati personali verso paesi terzi (WP12)[2]. In seguito all'entrata in vigore del regolamento generale dell'UE sulla protezione dei dati ("regolamento")[3], che ha sostituito la direttiva, il Gruppo sta rivedendo il documento WP12, contenente i suoi precedenti orientamenti, per aggiornarlo alla luce della nuova legislazione e della giurisprudenza recente della Corte di giustizia dell'Unione europea ("Corte")[4].

Il presente documento di lavoro si prefigge di aggiornare il capitolo 1 del WP12, relativo alla questione centrale del livello adeguato di protezione dei dati in un paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo o un'organizzazione internazionale (di seguito: "paesi terzi o organizzazioni internazionali"). Nei prossimi anni il documento sarà sottoposto a continue revisioni e, se necessario, aggiornato sulla base dell'esperienza pratica maturata grazie all'applicazione del regolamento. I capitoli 2 (*Applicazione dei principi ai paesi che hanno ratificato la convenzione n. 108 del Consiglio d'Europa*) e 3 (*Applicazione dei principi all'autodisciplina settoriale*) del documento WP12 dovrebbero essere aggiornati in una fase successiva.

Il presente documento di lavoro riguarda soltanto le decisioni di adeguatezza, che sono atti di esecuzione[5] della Commissione europea a norma dell'articolo 45 del regolamento. Altri aspetti dei trasferimenti di dati personali verso paesi terzi e organizzazioni internazionali saranno esaminati in successivi documenti di lavoro che saranno pubblicati separatamente (norme vincolanti d'impresa, deroghe).

Il presente documento mira a fornire orientamenti alla Commissione europea e al Gruppo, nel quadro del regolamento, per quanto concerne la valutazione del livello di tutela dei dati nei paesi terzi e nelle organizzazioni internazionali, stabilendo i principi fondamentali per la protezione dei dati che devono essere presenti nella legislazione di un paese terzo o in un'organizzazione internazionale per garantire un'equivalenza sostanziale con il quadro dell'UE. Inoltre, può fornire orientamenti ai paesi terzi e alle organizzazioni internazionali interessati a ottenere l'adeguatezza. Tuttavia, i principi delineati nel presente documento di lavoro non sono direttamente rivolti ai titolari del trattamento o ai responsabili del trattamento.

Il presente documento consta di 4 capitoli:

Capitolo 1: Alcune informazioni generali sul concetto di adeguatezza

Capitolo 2: Aspetti procedurali per i riscontri relativi all'adeguatezza a norma del regolamento

Capitolo 3: Principi generali di protezione dei dati. Questo capitolo contiene i principi generali fondamentali di protezione dei dati per garantire che il livello di protezione dei dati in un paese terzo o un'organizzazione internazionale sia sostanzialmente equivalente a quello stabilito dalla legislazione dell'UE.

Capitolo 4: Garanzie sostanziali per l'accesso a fini di contrasto e di sicurezza nazionale allo scopo di limitare le ingerenze nei diritti fondamentali. Il capitolo riporta le garanzie sostanziali per l'accesso a fini di contrasto e di sicurezza nazionale alla luce della sentenza Schrems del 2015 della Corte e sulla base del documento di lavoro sulle garanzie sostanziali adottato dal Gruppo nel 2016.

---

[1] Istituito in virtù dell'articolo 29 della direttiva 95/46/CE relativa alla tutela dei dati.

[2] WP12 "Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati", adottato dal Gruppo il 24 luglio 1998.

[3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)

[4] Compresa la sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner

[5] Cfr. l'articolo 45, paragrafo 3, e l'articolo 93, paragrafo 2, del regolamento per ulteriori informazioni sugli atti di esecuzione.

Capitolo 1: Alcune informazioni generali sul concetto di adeguatezza

L'articolo 45, paragrafo 1, del regolamento stabilisce il principio che i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono ammessi soltanto se il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato.

Questo concetto di "livello di protezione adeguato", che era già presente nella direttiva 95/46, è stato ulteriormente sviluppato dalla Corte. A questo proposito è importante richiamare il principio stabilito dalla Corte nella causa Schrems, secondo cui il "*livello di protezione*" nel paese terzo deve essere "*sostanzialmente equivalente*" a quello garantito all'interno dell'Unione, ma "*gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione*"[6]. Pertanto, l'obiettivo non è riprodurre punto per punto la legislazione europea, bensì stabilire i requisiti sostanziali - di base - di tale legislazione.

Scopo delle decisioni di adeguatezza da parte della Commissione europea è confermare formalmente con effetto vincolante per gli Stati membri[7] che il livello di protezione dei dati in un paese terzo o in un'organizzazione internazionale è sostanzialmente equivalente al livello di protezione dei dati all'interno dell'Unione europea[8]. L'adeguatezza può essere conseguita anche attraverso una combinazione di diritti degli interessati e obblighi in capo a chi effettua il trattamento o esercita il controllo sul trattamento, e il controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono azionabili e sono rispettate nella pratica. È pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti in un paese terzo o un'organizzazione internazionale, ma anche il sistema in atto per garantirne l'efficacia. La presenza di meccanismi di applicazione efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati.

L'articolo 45, paragrafo 2, del regolamento stabilisce gli elementi che la Commissione europea deve prendere in considerazione nel valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale.

Per esempio, la Commissione deve prendere in considerazione lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti e gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale.

È chiaro dunque che qualsiasi analisi significativa dell'adeguatezza della protezione deve comprendere due elementi fondamentali: il contenuto delle norme applicabili e i mezzi per garantirne l'effettiva applicazione. Spetta alla Commissione europea verificare sistematicamente che le norme in vigore siano efficaci nella pratica.

Il "nucleo" dei principi di contenuto in materia di protezione dei dati e delle prescrizioni di "procedura/applicazione", la cui osservanza potrebbe essere considerata una condizione minima di adeguatezza della protezione, è tratto dalla Carta dei diritti fondamentali dell'Unione europea e dal regolamento. È inoltre opportuno prendere in considerazione altri accordi internazionali in materia di protezione dei dati, per esempio la convenzione n. 108[9].

Occorre prestare attenzione altresì al quadro giuridico per l'accesso delle autorità pubbliche ai dati personali. Ulteriori orientamenti in materia sono reperibili nel documento di lavoro 237 (il documento sulle garanzie sostanziali)[10] sulle garanzie nel contesto della sorveglianza.

---

[6] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punti 73-74).

[7] Articolo 288, paragrafo 2, TFUE.

[8] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 52).

[9] Considerando 105 del regolamento.

[10] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) [Documento di lavoro 01/2016 sulla giustificazione delle ingerenze nei diritti fondamentali alla vita privata e alla protezione dei dati tramite

Le disposizioni generali sulla protezione dei dati e la vita privata nel paese terzo non sono sufficienti. Nel quadro giuridico del paese terzo o dell'organizzazione internazionale devono figurare disposizioni specifiche che rispondono a necessità concrete correlate ad aspetti pratici rilevanti del diritto alla protezione dei dati. Tali disposizioni devono essere vincolanti.

Capitolo 2: Aspetti procedurali per i riscontri relativi all'adeguatezza a norma del regolamento

Per poter adempiere al proprio compito di fornire consulenza alla Commissione europea a norma dell'articolo 70, paragrafo 1, lettera s), del regolamento, il comitato europeo per la protezione dei dati ("comitato") deve ricevere la documentazione necessaria, compresa la corrispondenza pertinente e le conclusioni tratte dalla Commissione europea. Se il quadro giuridico è complesso, dovrebbero essere fornite anche eventuali relazioni sul livello di protezione dei dati nel paese terzo o nell'organizzazione internazionale. In ogni caso, le informazioni fornite dalla Commissione europea dovrebbero essere esaustive e permettere al comitato di effettuare la valutazione del livello di protezione dei dati nel paese terzo. Il comitato fornirà in tempo utile un parere sui riscontri della Commissione europea e individuerà eventuali carenze nel quadro giuridico in materia di adeguatezza. Il comitato inoltre si adopererà per proporre variazioni o modifiche per ovviare alle eventuali carenze.

A norma dell'articolo 45, paragrafo 4, del regolamento, spetta alla Commissione controllare su base continuativa gli sviluppi che potrebbero incidere sul funzionamento delle decisioni di adeguatezza.

L'articolo 45, paragrafo 3, del regolamento stabilisce che deve essere effettuato un riesame periodico almeno ogni quattro anni. Si tratta di un'indicazione temporale generica, che deve essere adattata a ciascun paese terzo o a ciascuna organizzazione internazionale tramite una decisione di adeguatezza. A seconda delle circostanze particolari del caso, potrebbe essere giustificata una frequenza più breve. Inoltre, un incidente o nuove informazioni sul quadro giuridico del paese terzo o dell'organizzazione internazionale o una modifica dello stesso potrebbero rendere necessario anticipare il riesame rispetto al previsto. Sarebbe inoltre opportuno procedere tempestivamente a un primo riesame di una decisione di adeguatezza interamente nuova e adattare progressivamente il ciclo di riesame in base all'esito di tale attività.

Alla luce dell'obbligo del comitato di fornire alla Commissione un parere per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione, il comitato deve ricevere a tempo debito dalla Commissione europea informazioni significative sul monitoraggio degli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale in questione. Il comitato dovrebbe quindi essere tenuto informato su eventuali processi di riesame e missioni di valutazione in corso nel paese terzo o con riferimento all'organizzazione internazionale. Il comitato apprezzerebbe un invito a partecipare a tali processi di riesame e missioni di valutazione.

Va inoltre rilevato che, a norma dell'articolo 45, paragrafo 5, del regolamento, la Commissione europea ha il diritto di revocare, modificare o sospendere le decisioni di adeguatezza in vigore. La procedura per revocare, modificare o sospendere le decisioni di adeguatezza dovrebbe conseguentemente coinvolgere il comitato, cui dovrebbe essere richiesto un parere a norma dell'articolo 70, paragrafo 1, lettera s).

In aggiunta, come ora previsto dall'articolo 58, paragrafo 5, del regolamento e in base a quanto stabilito dalla sentenza Schrems della Corte, le autorità di protezione dei dati devono poter intentare un'azione legale ove ritengano fondate le censure sollevate da una persona nei confronti di una decisione di adeguatezza: *"[...] incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di*

misure di sorveglianza durante i trasferimenti di dati personali (Garanzie sostanziali europee)], 16/EN WP 237, 13 aprile 2016.

tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione" [11].

[11] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 65).

Capitolo 3: Principi generali di protezione dei dati per garantire che il livello di protezione in un paese terzo, un territorio o uno o più settori specifici all'interno di tale paese terzo, o in un'organizzazione internazionale sia sostanzialmente equivalente a quello garantito dalla legislazione dell'UE

Il sistema di un paese terzo o di un'organizzazione internazionale deve contenere i seguenti principi di contenuto e meccanismi di procedura/applicazione basilari:

A. <u>Principi di contenuto:</u>

1) Nozioni

Dovrebbero essere presenti nozioni e/o principi basilari in materia di protezione dei dati. Tali nozioni e principi non devono necessariamente riprendere la terminologia del regolamento, ma dovrebbero rispecchiare ed essere coerenti con le nozioni racchiuse nel diritto europeo in materia di protezione dei dati. A titolo esemplificativo, il regolamento contiene le seguenti nozioni fondamentali: "dati personali", "trattamento di dati personali", "titolare del trattamento", "responsabile del trattamento", "destinatario" e "dati sensibili".

2) Criteri di liceità e correttezza del trattamento per fini legittimi

I dati devono essere trattati in modo lecito, corretto e legittimo.

Le basi di legittimità che consentono il trattamento lecito, corretto e legittimo dei dati personali dovrebbero essere definite in maniera sufficientemente chiara. Il quadro europeo riconosce alcuni criteri di legittimità tra cui, per esempio, le disposizioni del diritto nazionale, il consenso dell'interessato, l'esecuzione di un contratto o il legittimo interesse del titolare del trattamento o di un terzo a condizione che non prevalgano gli interessi dell'interessato.

3) Il principio della finalità limitata

I dati dovrebbero essere trattati per una finalità specifica e successivamente utilizzati soltanto nella misura in cui non vi sia incompatibilità con la finalità del trattamento.

4) Il principio della qualità e della proporzionalità

I dati dovrebbero essere precisi e aggiornati laddove necessario. I dati dovrebbero essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite.

5) Il principio della conservazione dei dati

Di norma i dati dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

6) Il principio della sicurezza e della riservatezza

Qualsiasi organismo incaricato del trattamento dei dati dovrebbe assicurare che questi siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Il livello di sicurezza dovrebbe tenere in considerazione lo stato dell'arte e i relativi costi.

7) Il principio di trasparenza

Ogni persona dovrebbe essere informata in merito a tutti i principali elementi del trattamento dei dati personali che la riguardano in forma chiara, facilmente accessibile, concisa, trasparente e di facile comprensione. Tali informazioni dovrebbero includere la finalità del trattamento, l'identità del titolare del trattamento, i diritti di cui gode e altre informazioni, purché ciò sia necessario a garantire la correttezza. A determinate condizioni, sono ammesse alcune eccezioni a tale diritto di informazione, ad esempio per salvaguardare le indagini penali, la sicurezza nazionale, l'indipendenza della magistratura e dei procedimenti giudiziari o altri importanti obiettivi di interesse pubblico generale, come nel caso dell'articolo 23 del regolamento.

8) I diritti di accesso, rettifica, cancellazione e opposizione

L'interessato dovrebbe avere il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e l'accesso a tali dati, compresa una copia di tutti i dati trattati che lo riguardano.

L'interessato dovrebbe avere il diritto di ottenere la rettifica dei dati che lo riguardano, per motivi specifici, ad esempio ove siano palesemente inesatti o incompleti, nonché la loro cancellazione, ad esempio quando il trattamento non è più necessario o è illecito.

L'interessato dovrebbe inoltre avere il diritto di opporsi in qualsiasi momento, per motivi legittimi cogenti relativi alla sua situazione particolare, al trattamento dei dati che lo riguardano a determinate condizioni previste dalla legislazione del paese terzo. Il regolamento, ad esempio, prevede tra tali condizioni il caso in cui il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento o il caso in cui il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

L'esercizio di tali diritti non dovrebbe essere eccessivamente oneroso per l'interessato. Si potrebbero prevedere eventuali limitazioni a tali diritti, ad esempio per salvaguardare le indagini penali, la sicurezza nazionale, l'indipendenza della magistratura e dei procedimenti giudiziari o altri importanti obiettivi di interesse pubblico generale, come nel caso dell'articolo 23 del regolamento.

9) Restrizioni ai trasferimenti successivi

Ulteriori trasferimenti dei dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentiti soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento. Il livello di tutela delle persone fisiche i cui dati sono trasferiti non deve essere compromesso dal trasferimento successivo. Spetta al primo destinatario dei dati trasferiti dall'UE assicurare che siano previste garanzie adeguate per i trasferimenti successivi dei dati in mancanza di una decisione di adeguatezza. Tali trasferimenti successivi di dati dovrebbero essere possibili soltanto per finalità determinate e limitate e purché sussista una base giuridica per il trattamento.

B. <u>Esempi di principi di contenuto supplementari da applicare in casi specifici di trattamento:</u>

1) Categorie particolari di dati

Dovrebbero esistere garanzie specifiche nel caso in cui siano interessate "categorie particolari" di dati[12]. Tali categorie dovrebbero riflettere quelle previste agli articoli 9 e 10 del regolamento. La protezione dovrebbe essere messa in atto tramite l'introduzione di requisiti di trattamento più severi, ad esempio il fatto che l'interessato fornisca il suo consenso esplicito al trattamento o tramite misure di sicurezza supplementari.

2) Marketing diretto

Se il trattamento dei dati avviene per finalità di marketing diretto, l'interessato dovrebbe essere in grado, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento con riferimento ai dati che lo riguardano.

3) Processo decisionale automatizzato, compresa la profilazione

Le decisioni basate unicamente sul trattamento automatizzato (processo decisionale automatizzato relativo alle persone fisiche), compresa la profilazione, che producono effetti giuridici che riguardano l'interessato o incidono significativamente sulla sua persona sono ammesse soltanto a determinate condizioni stabilite dal quadro giuridico del paese terzo. Nel quadro europeo tali condizioni comprendono, per esempio, la necessità di ottenere il consenso esplicito dell'interessato o la necessità di tale decisione per la conclusione di un contratto. Se la decisione non è conforme alle condizioni stabilite dal quadro giuridico del paese terzo, l'interessato dovrebbe avere il diritto di non essere sottoposto alle sue prescrizioni. Il diritto del paese terzo dovrebbe, in ogni caso, prevedere le necessarie garanzie, compreso il diritto a essere informato sui motivi particolari sottesi alla decisione e sulla sua logica, a rettificare informazioni inaccurate o incomplete e a contestare la decisione qualora questa sia stata adottata sulla base di un fondamento di fatto errato.

C. <u>Meccanismi di procedura e applicazione</u>

Anche se gli strumenti dei quali il paese terzo si avvale per assicurare un livello di protezione adeguato possono essere diversi da quelli attuati all'interno dell'Unione europea[13], un sistema coerente con quello europeo deve essere caratterizzato dalla presenza dei seguenti elementi:

1) Autorità di controllo competenti indipendenti

Nel paese terzo dovrebbero essere presenti una o più autorità di controllo indipendenti, con il compito di monitorare, garantire e far rispettare le disposizioni in materia di protezione dei dati e della vita privata. L'autorità di controllo agisce in piena indipendenza e imparzialità nell'adempimento dei suoi compiti e nell'esercizio dei suoi poteri, senza richiedere né accettare istruzioni. In tale contesto, l'autorità di controllo dovrebbe disporre di tutti i necessari poteri e incarichi disponibili per garantire la conformità ai diritti in materia di protezione dei dati e per sensibilizzare l'opinione pubblica al riguardo. Dovrebbero inoltre essere presi in considerazione il personale e il bilancio dell'autorità di controllo. L'autorità di controllo dovrebbe essere in grado, infine, di condurre indagini di propria iniziativa.

2) Il sistema di protezione dei dati deve garantire un buon livello di conformità

Il sistema di un paese terzo dovrebbe garantire un buon livello di responsabilizzazione e di consapevolezza dei propri obblighi, compiti e responsabilità tra i titolari del trattamento e tra chi si occupa, per conto loro, del trattamento dei dati personali, e dei propri diritti e dei mezzi a disposizione

[12] Tali categorie particolari sono dette anche "dati sensibili" al considerando 10 del regolamento.

[13] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 74).

per l’esercizio degli stessi tra gli interessati. L’esistenza di sanzioni effettive e dissuasive può svolgere un ruolo importante nel garantire il rispetto delle norme, così come la presenza di sistemi di verifica diretta da parte di autorità, ispettori o addetti indipendenti alla protezione dei dati.

3) **Responsabilizzazione**

Il quadro giuridico per la protezione dei dati di un paese terzo dovrebbe obbligare i titolari del trattamento e/o i soggetti che trattano i dati personali per loro conto a rispettarne le disposizioni e a fornire le prove di tale conformità, in particolare all’autorità di controllo competente. Tali misure potrebbero comprendere, per esempio, valutazioni dell’impatto della protezione dei dati, la tenuta di registri o file di log delle attività di trattamento dei dati per un periodo di tempo adeguato, la nomina di un addetto alla protezione dei dati o la protezione dei dati fin dalla progettazione e la protezione dei dati di default.

4) **Il sistema di protezione dei dati deve fornire aiuto e sostegno agli interessati nell’esercizio dei loro diritti nonché meccanismi di ricorso appropriati**

L’interessato dovrebbe essere in grado di avvalersi di mezzi di ricorso per far valere i propri diritti con rapidità ed efficacia, e senza costi proibitivi, nonché per garantire la conformità. A tal fine devono essere disponibili meccanismi di controllo che consentano un’indagine indipendente sulle denunce e che permettano di individuare e sanzionare nella pratica eventuali violazioni del diritto alla protezione dei dati e al rispetto della vita privata.

In caso di inosservanza delle norme, all’interessato dovrebbe inoltre essere riconosciuto un mezzo di ricorso effettivo in sede amministrativa e giudiziale, anche ai fini del risarcimento per i danni subiti a causa di un trattamento illecito dei dati personali che lo riguardano. Si tratta di un elemento fondamentale che deve prevedere un sistema di valutazione o arbitrato indipendenti che permettano il pagamento di un risarcimento e l’imposizione di sanzioni, se del caso.

Capitolo 4: Garanzie sostanziali nei paesi terzi per l'accesso a fini di contrasto e di sicurezza nazionale allo scopo di limitare le ingerenze nei diritti fondamentali

A norma dell'articolo 45, paragrafo 2, lettera a), del regolamento, nel valutare l'adeguatezza del livello di protezione la Commissione prende in considerazione "*la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione [...]*".

La Corte, nella sentenza Schrems, ha osservato che "*l'espressione 'livello di protezione adeguato' deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta"*. Anche se gli strumenti dei quali il paese terzo si avvale, al riguardo, possono essere diversi da quelli attuati all'interno dell'Unione, tali strumenti devono cionondimeno rivelarsi efficaci nella prassi[14].

A tale proposito, la Corte ha anche osservato in tono critico che la precedente decisione "Safe Harbor" "*non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale*".

Il Gruppo ha individuato nel parere WP237, adottato il 13 aprile 2016, garanzie sostanziali che rispecchiano la giurisprudenza della Corte e della CEDU in tema di controlli. Se è vero che le raccomandazioni formulate nel parere WP237 rimangono valide, e dovrebbero essere prese in considerazione nel valutare l'adeguatezza di un paese terzo per quanto concerne i controlli, altrettanto certo è che l'applicazione di tali garanzie può differire nei settori dell'accesso ai dati a fini di contrasto e di sicurezza nazionale. Tuttavia, per accedere ai dati a fini di contrasto o di sicurezza nazionale tutti i paesi terzi devono rispettare le seguenti quattro garanzie per essere considerati adeguati:

1) **Il trattamento dovrebbe essere fondato su norme chiare, precise e accessibili (base giuridica)**

2) **È necessario dimostrare la necessità e la proporzionalità degli obiettivi legittimi perseguiti**

3) **Il trattamento deve essere sottoposto a controlli indipendenti**

4) **Gli interessati devono avere a disposizione mezzi di ricorso effettivi**

[14] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 74).