Allegato TiSA filtrato sul Commercio Elettronico

Analisi di Burcu Kilic, *Public Citizen*

& Tamir Israel, *Canadian Internet Policy & Public Interest Clinic*

Oggi WikiLeaks ha pubblicato una bozza aggiornata dell'Allegato sul Commercio Elettronico del proposto Accordo sul Commercio di Servizi (TiSA). Il TiSA è un accordo commerciale attualmente in corso di negoziazione tra 23 paesi (contando la UE come uno) che si autodefiniscono "i Veri Buoni Amici dei Servizi".

L'Allegato sul commercio elettronico include misure sostenute dagli Stati Uniti sul commercio elettronico, il trasferimento di tecnologie, i flussi transnazionali di dati e la neutralità della rete che amplierebbero l'ambito e le regole dell'Accordo Generale del Commercio di Servizi (GATS) presso l'Organizzazione Mondiale del Commercio (WTO).

Il TiSA è inteso come un accordo pari a un "regime aureo" cui altri paesi possono accedere, che fissa nuovi parametri che informeranno altri accordi e alla fine sarà re-incorporato nel GATS per essere applicato a tutti i membri della WTO.

Norme selezionate

Articolo 2: Trasferimenti di informazioni o flussi transnazionali di informazioni

Articolo 2: [CA/PE/US propongono: Trasferimenti di Informazioni] [JP/MX/CH propongono: Flussi Transnazionali di Informazioni]

[**KR**: Riguardo all'articolo sui trasferimenti di informazioni la Corea è del parere che qualsiasi trasferimento di informazioni originato dall'attività di un fornitore di servizi debba essere basato sul "consenso informato". Il consenso informato si riferisce all'idea che gli individui che forniscono loro informazioni personali a fornitori di servizi debbano godere della piena protezione e del diritto di ricorso assicurati dalla legge per quanto riguarda l'utilizzo delle loro informazioni personali fornite a fornitori di servizi. Ciò dovrebbe essere appropriatamente riflesso nella formulazione dell'articolo.

HK: Il trasferimento di informazioni non dovrebbe arrecare pregiudizio al regime nazionale per la protezione di dati personali e dovrebbe essere basato sul consenso informato.]

1. [**CA/TW/CO/JP/MX/US propongono**: Nessuna Parte può impedire a un fornitore di servizi di un'altra Parte [**CO/JP propongono**: o a utenti di tali fornitori,] [**CA/CO/JP/TW/US propongono**: di trasferire, [accedere, elaborare o archiviare] informazioni, comprese informazioni personali, all'interno o all'esterno del territorio della Parte in cui tale attività è condotta in rapporto con la conduzione degli affari del fornitore di servizi.]

2. [**US propongono**: SEGNAPOSTO per le istituzioni finanziarie.]

3. [**CH propone: CO si oppone**: Le Parti dovrebbero avere misure per proteggere i consumatori coinvolti nel commercio elettronico da pratiche commerciali fraudolente o ingannevoli.]

4. [**CH propone; CO si oppone**: Le Parti dovrebbero rafforzare la loro capacità di controllo per assicurare che siano rispettate le leggi e i regolamenti applicabili concernenti la protezione dei dati e la riservatezza.]

5. [**CH propone; CO/US si oppongono**: Le Parti non dovrebbero impedire a fornitori stranieri di commercio elettronico o a clienti di tali fornitori di trasferire elettronicamente informazioni all'interno o a livello transnazionale, di accedere a informazioni pubblicamente disponibili o di accedere alle proprie informazioni archiviate all'estero.]

Le Parti stanno dibattendo il titolo di questa clausola in cui Canada, Peru e Stati Uniti propongono "trasferimenti di informazioni" e Giappone, Messico e Cina [rectius: Svizzera – n.d.t.] propongono "flussi transnazionali di informazioni". Un possibile motivo di questo dibattito è che "trasferimento di informazioni" [o "libero flusso di informazioni"] suona più amichevole e collegato ai diritti umani. "Flussi transnazionali di informazioni" suona più orientato al commercio.

L'Articolo 2.1 propone che "Nessuna Parte possa impedire il trasferimento, l'accesso, l'elaborazione e l'archiviazione di informazioni (comprese informazioni personali) all'esterno del territorio della Parte se condotti in rapporto con un'attività commerciale". Questa norma agevola i trasferimenti transnazionali di dati e la loro elaborazione in tutti i settori dei servizi, compresi i servizi finanziari, senza limitazioni.

Le leggi sulla protezione dei dati esistono per trovare un compromesso tra i diritti degli individui alla riservatezza e la capacità delle imprese di utilizzare i dati ai fini delle loro attività. Questa norma garantisce alle imprese libertà sul modo in cui utilizzano i dati (comprese informazioni personali) senza che esse siano assoggettate a restrizioni. I governi possono non essere in grado di garantire che i dati siano elaborati equamente e legalmente o ottenuti solo per scopi specificati e legali. Poiché non ci sarà controllo sui dati, non sarà possibile verificare se i dati sono conservati più a lungo di quanto necessario o per gli scopi per cui sono elaborati. Non è chiaro che cosa accadrebbe nel caso di elaborazioni non autorizzati o illegali, o di perdite o distruzioni accidentali, o danneggiamenti, di dati personali. Questa norma consente il trasferimento transnazionale di dati in un paese o territorio senza conferma che il paese abbia un livello adeguato di protezione dei diritti e delle libertà degli individui.

La Corea vuole che i trasferimenti transnazionali di dati di fornitori di servizi siano basati sul "consenso informato". Il consenso informato disciplina certi tipi di comunicazioni tra fornitori di servizi e utenti riguardo all'utilizzo delle loro informazioni personali.

La norma proposta dalla Svizzera prevede il trasferimento transnazionale di informazioni nell'ambito di reti nazionali o all'estero.

Articolo 3: Protezione dei consumatori in rete

Articolo 3: Protezione dei Consumatori in Rete

[**CH** preferisce utilizzare "commercio elettronico" piuttosto che "attività commerciali in rete".]

1. [**AU/CA/CL/TW/C0/UE/HK/IS/IL/JP/KR/LI/MX/NZ/NO/PA/PE propongono:** Le Parti riconoscono l'importanza di mantenere e adottare misure trasparenti ed efficaci per proteggere i consumatori da attività commerciali fraudolente o ingannevoli] [**CO/JP/MX propongono:** , nonché misure che contribuiscano allo sviluppo della fiducia dei consumatori,] quando operano nel commercio elettronico].

2. [**AU/CA/CL/TW/CO/UE/HK/IS/IL/JP/KR/LI/MX/NZ/NO/PA/PE propongono:** A questo fine ciascuna Parte adotterà o manterrà leggi per la protezione dei consumatori per vietare attività commerciali fraudolente o ingannevoli che [possano danneggiare] [possano danneggiare o potenzialmente danneggiare] consumatori che utilizzino il [**CO propone:** commercio elettronico] [**AU/CL/JP/KR/NZ/PE propongono:** attività commerciali in rete].

3. **[CO propone:** Sulla base di termini e condizioni non discriminanti ciascuna Parte assicurerà ai consumatori che utilizzano il commercio elettronico con i propri [? – n.d.t.] fornitori di servizi l'accesso ai meccanismi esistenti di protezione dei consumatori messi a disposizione dalle rispettive autorità nazionali di protezione dei consumatori].

4. [**AU/CL/CO/JP/MX/NZ/PE propongono:** Le Parti **[AU/CL/JP/MX/NZ/PE propongono:** riconoscono l'importanza della] [**CO propone:** si sforzeranno di promuovere la] cooperazione tra le loro rispettive agenzie o altri organismi nazionali di protezione dei consumatori su attività collegate al commercio elettronico [**AU/CL/NZ/PE propongono:** transnazionale] al fine di accrescere [il bene] [**MX propone:** la fiducia] dei consumatori].

5. [**CO/MX propongono:** Le Parti, in conformità con le proprie leggi e regolamenti, consentiranno alle persone di decidere mutuamente i metodi appropriati per risolvere le controversie scaturenti da transazioni di commercio elettronico. Tali metodi possono includere, senza esservi limitati, meccanismi di

risoluzione in rete delle dispute.]

La sub-clausola 5 dell'Articolo 3 fa sorgere specifiche preoccupazioni riguardo a una caratteristica comune e importante di molte leggi per la protezione dei consumatori. Questa clausola vieta ai governi di interferire in tentativi individuali di "decidere mutuamente i metodi appropriati per risolvere le controversie scaturenti da transazioni di commercio elettronico ... include[ndo] … meccanismi di risoluzione in rete delle dispute". Numerose cornici di protezione dei consumatori hanno adottato divieti dell'uso di clausole di risoluzione delle dispute in contratti con i consumatori. La spinta all'origine di tale norma è che tali clausole sono spesso imposte unilateralmente in contratti di adesione dei consumatori e utilizzate per prevenire efficacemente qualsiasi accesso ai tribunali e, in particolare, a meccanismi di azione collettiva per il riconoscimento, complessivamente, di rivendicazioni limitate. Tuttavia l'articolo 3.5 sembrerebbe precludere l'utilizzo di norme che garantiscono l'accesso ai tribunali e a meccanismi di azione collettiva, poiché ciò costituirebbe un'interferenza in meccanismi di risoluzione delle controversie mutuamente decisi nonostante la realtà di tale "accordo" dei consumatori sia sotto forma di clausole non negoziabili in contratti di adesione più generali.

Articolo 4: Protezione delle informazioni personali

Articolo 4: Protezione delle Informazioni Personali

1. [**AU/CA/CL/TW/CO/IL/JP/KR/MX/NZ/NO/PA/PE propongono:** La Parti riconoscono i benefici economici e sociali della protezione delle informazioni personali degli utenti del commercio elettronico e il contributo che essa offre al rafforzamento della fiducia dei consumatori nel commercio elettronico.]

2. [**AU/CA/CL/TW/CO/IL/KR/MX/NZ/NO/PA/PE propongono:** A questo fine ciascun Parte adotterà o manterrà un quadro legale nazionale che preveda la protezione delle informazioni personali degli utenti del commercio elettronico. Nello sviluppo di questi quadri di protezione delle informazioni personali ciascuna Parte dovrebbe tener conto dei principi e delle linee guida degli organi internazionali relativi.]

[**CA propone:** Ciascuna parte assicurerà che il suo quadro legale nazionale per la protezione delle informazioni personali degli utenti del commercio elettronico sia applicato su basi non discriminanti.]

3. [**AU/CA/CL/TW/CO/IL/JP/KR/MX/NZ/NO/PA/PE propongono:** Ciascuna Parte dovrebbe pubblicare informazioni sulla protezione delle informazioni personali che offre agli utenti del commercio elettronico, tra cui:

a) come le persone possono perseguire rimedi, e
b) come le imprese possono rispettare le prescrizioni legali.]

Le Parti riconoscono i benefici economici e sociali della protezione dei dati personali degli utenti del commercio elettronico ed è loro richiesto di adottare o mantenere un quadro legale nazionale che offra la protezione delle informazioni personali degli utenti del commercio elettronico. A questo fine una maggioranza delle parti negoziatrici propone che le leggi nazionali che proteggono le informazioni personali debbano seguire i principi e le linee guida degli organi internazionali relativi. Non è probabile, ad esempio, che gli Stati Uniti adottino una 'legge' o una serie di leggi sulla riservatezza, ma continueranno ad affidarsi a norme ad hoc della FTC [Commissione Federale sul Commercio – n.d.t.] e a regole di condotta volontarie.

Il Canada propone una base non discriminatoria per la protezione delle informazioni personali. Rimarchevolmente assenti sono gli Stati Uniti. Gli Stati Uniti non prendono posizione sulla

protezione delle informazioni personali. Ciò può essere dovuto al fatto che gli Stati Uniti non hanno una singolo sistema generale per proteggere le informazioni personali. Hanno invece un mosaico di leggi federali e statali e norme per la raccolta e l'utilizzo di dati personali che possono sovrapporsi, connettersi e possono contraddirsi tra loro.

Articolo 5: Comunicazioni elettroniche commerciali non richieste

Articolo 5: [AU/CO/NZ propongono: Messaggi][UE propone; NO considera: Comunicazioni] Elettroniche Commerciali Non Richieste

1. **[AU/CA/CL/CO/CR/UE/IL/JP/KR/MX/NZ/NO/PE propongono:** Ciascuna Parte [**TW/TR propongono:** si sforzerà di] adotterà o manterrà misure concernenti [messaggi] [**UE propone:** comunicazioni] elettroniche commerciali non richieste che:]

a) prescrivano ai fornitori di messaggi elettronici commerciali non richiesti di agevolare la capacità dei destinatari di bloccare tali messaggi; or [**UE/NO propongono; AU si oppone:** e]

b) prescrivano il consenso, come specificato in base alle leggi e ai regolamenti di ciascuna Parte, dei destinatari a ricevere messaggi elettronici commerciali; [**UE/NO si oppongono:** o

c) altrimenti provvedano alla minimizzazione dei messaggi elettronici non richiesti.]]

2. **[AU/CA/CL/CO/IL/JP/KR/NZ/NO/PE propongono:** Ciascuna Parte [**TW/TR propongono:** si sforzerà di] assicurerà ricorso contro fornitori di messaggi elettronici commerciali non richiesti che non rispettino le proprie misure messe in atto in forza del paragrafo 1.]

3. [**AU/CA/CL/CO/CR/UE/IL/KR/JP/NZ/NO/PE propongono:** Le Parti si sforzeranno di cooperare nei casi di mutuo interesse riguardanti la disciplina dei messaggi elettronici commerciali non richiesti.]

L'Articolo 5 prescrive che le Parti adottino misure che disciplinino le comunicazioni elettroniche commerciali non richieste. La sub-clausola a) propone un'opzione di rifiuto in cui un destinatario può bloccare i messaggi. La sub-clausola b) propone che comunicazioni commerciali non richieste richiedano che l'utente dia il proprio consenso o scelga di aderire. Inoltre la sub-clausola c) propone l'adozione di altre misure che minimizzerebbero i messaggi commerciali non richiesti.

Attualmente queste tre misure sono presentate come opzioni alternative, lasciando ai firmatari ampia libertà quanto al modo scelto per disciplinare la *spam* elettronica. Una proposta della UE di rendere le sub-clausole da a) a c) obblighi cumulativi rafforzerebbe considerevolmente la norma che, nella sua forma attuale, in realtà richiede soltanto alle Parti statali di "provvedere alla minimizzazione di messaggi elettronici commerciali non richiesti" in qualsiasi modo ritengano adatto. Se la proposta UE fosse adottata, tuttavia, numerosi dei regimi anti-spam esistenti dovranno essere considerevolmente rivisti per imporre l'obbligo di un consenso preventivo. Inoltre il TiSA cederebbe un livello di controllo sul modo in cui sono internazionalmente interpretati termini chiave relativi al controllo della *spam.*

Anche se l'Articolo 5 riserva espressamente ai governi nazionali la definizione del termine "consenso", non fa altrettanto riguardo a che cosa possa significare in questo contesto la garanzia agli utenti finali del diritto di bloccare i messaggi.

Articolo 6 – Trasferimento dell'accesso al codice sorgente

Articolo 6: [JP propone; CO si oppone: Trasferimento o Accesso al Codice Sorgente

1. Nessuna Parte può richiedere il trasferimento del, o l'accesso al, codice sorgente di software di proprietà di un'altra Parte come condizione per offrire servizi collegati a tale software nel proprio

territorio.

2. Ai fini di questo Articolo, il software disciplinato dal paragrafo 1 è limitato al software del mercato di massa e non include il software utilizzato per infrastrutture critiche.]

La proposta del Giappone mira a vietare che i governi richiedano a una società che offra un servizio collegato a software di trasferire o fornire accesso al codice sorgente del software. Le infrastrutture critiche sono categoricamente esentate da tale divieto.

Così come nel caso di molte altre parti dell'allegato al TiSA sul commercio elettronico, questa norma è mal concepita e a un tempo eccessivamente e insufficientemente inclusiva. Ci sono molte situazioni diverse dal contesto delle infrastrutture critiche in cui potrebbe essere desiderabile in una prospettiva di politica pubblica richiedere accesso a software, ad esempio nel caso dei router degli utenti la cui scarsa sicurezza costituisce un continuo problema per le reti domestiche. Un divieto non sfumato e categorico di richiedere l'accesso al codice sorgente può pregiudicare la trasparenza e l'utilizzo delle offerte di codice sorgente negli appalti governativi. Un governo che richieda la pubblicazione del codice sorgente come condizione essenziale di una proposta di servizio – un meccanismo che promuoverebbe la trasparenza pubblica dei servizi governativi e incoraggerebbe in generale l'uso del codice aperto – potrebbe essere facilmente interpretato come una violazione dell'Articolo 6 da ogni fornitore di servizi che desideri mantenere proprietario il proprio codice sorgente.

D'altro canto il divieto dell'Articolo 6 può anche essere insufficientemente inclusivo. Potrebbero esserci buoni motivi per impedire che un particolare governo abbia accesso al codice sorgente di software utilizzato in infrastrutture critiche. Per offrire solo un esempio un regolatore potrebbe desiderare di imporre obblighi di revisione al fine di controllare le capacità di filtraggio o di controllo di strumenti di Deep Packet Inspection installati nella rete mobile o fissa di un fornitore di servizi. Ciò potrebbe essere necessario per comprendere attività potenziale invasive della riservatezza e censorie della rete.

Un approccio più calibrato alla disciplina dell'accesso al, o del trasferimento del, codice sorgente derogherebbe al divieto categorico del TiSA e codificherebbe invece obiettivi o finalità in base alle quali è o non è accettabile che tali condizioni siano imposte.

Art. 7 – Interoperabilità

Articolo 7: [CO propone: Interoperabilità]

[**CO propone:** Ciascuna parte si sforzerà di promuovere l'interoperabilità tra le proprie procedure governative in rete e i servizi offerti attraverso mezzi elettronici.]

La proposta della Colombia mira ad assicurare interoperabilità tra le procedure governative in rete e i servizi offerti attraverso mezzi elettronici. Conseguire l'interoperabilità richiede tutela e consacrazione, in termini di attuazione pratica, di servizi a livello operativo in tutti i settori. Considerato che i "Veri Buoni Amici" dell'industria dei servizi sono privi dell'infrastruttura cooperativa di altri organismi di governo, quali l'OCSE, l'APEC e l'IGF, non è chiaro attraverso quale meccanismo intendano realizzare questo mandato.

Articolo 8 – Reti Aperte, Accesso alla Rete e suo Utilizzo

Articolo 8: Reti Aperte, Accesso alla Rete e suo Utilizzo

1. [**AU/CA/CL/CO/IL/JP/NO/PE/US propongono:** Ciascuna Parte riconosce che i consumatori nel suo territorio, subordinatamente alle leggi e ai regolamenti applicabili, dovrebbero essere in grado di:

a) accedere a, e utilizzare i, servizi e le applicazioni di loro scelta disponibili su Internet, nel rispetto di ragionevole amministrazione della rete;

b) collegare dispositivi di loro scelta a Internet, a condizione che tali dispositivi non danneggino la rete, e

c) avere accesso a informazioni sulle pratiche di gestione della rete del loro fornitore di accesso ai servizi Internet.]

2. [**KR si oppone [CO/CH propongono:** Le Parti, preferibilmente attraverso i regolatori relativi, dovrebbero promuovere la capacità dei consumatori di accedere, condividere e fornire legittimamente informazioni e di gestire applicazioni e di usare servizi di loro scelta] [**CO/JP propongono:** Ciascuna Parte si sforzerà di non [**TR propone:** senza pregiudizio per le leggi applicabili] [**CH propone:** le Parti non dovrebbero] [**CO,JP,CH propongono:** limitare la capacità] [**JP propone:** dei fornitori di servizi di fornire servizi][**CO,CH propongono:** di fornire servizi] [**CO/JP/CH propongono:** su Internet][**CH propone:** tra cui][**CO/JP/CH propongono:** su basi transnazionali e tecnologicamente neutre, e][**JP propone:** si sforzeranno di] [**CO/CH propongono:** dovrebbero][**CO/JP/CH propongono:** promuovere l'interoperabilità dei servizi e delle tecnologie, ove appropriato.][**JP propone:** Ciascuna Parte si sforzerà di assicurare che i fornitori di accesso a Internet evitino discriminazioni irragionevoli nel trasmettere traffico legale di rete.]]

Questa norma è molto simile all'Articolo X.5 della proposta statunitense datata 25 aprile 2014. Questo è un obbligo morbido celato nella formula del "riconoscimento" che i consumatori dovrebbero essere in grado di accedere a qualsiasi servizio o applicazione su Internet, a condizione di una gestione ragionevole della rete; di collegarvi qualsiasi dispositivo vogliano, a condizione che il farlo non danneggi la rete; e di accedere a informazioni sulle pratiche di gestione della rete di coloro che forniscono loro accesso a Internet.

La norma affronta la neutralità della rete in modo minimalistico e tuttavia, nonostante ciò, problematico. La sub-clausola 1 (a) dell'Articolo 8 impone un divieto di bloccare l'accesso al contenuto. La sub-clausola 1 (a) consente ai fornitori di bloccare l'accesso al contenuto a fini di "ragionevole amministrazione della rete". La ragionevole gestione della rete è un parametro molto più permissivo di quello adottato da altre giurisdizioni e può richiedere modifiche ai quadri esistenti di neutralità della rete. Non è chiaro come l'eccezione per la "ragionevole amministrazione della rete" del TiSA sarà alla fine interpretata da qualsivoglia organo di controllo sia alla fine adottato per far valere tali obblighi. E' interessante che l'espressione "ragionevole amministrazione della rete" non sia utilizzata nella norma equivalente dell'Articolo 15.7 del KORUS [Trattato di libero scambio tra USA e Corea – n.d.t.]. La sub-clausola 1(b), che vieta il blocco dall'accesso alla rete di dispositivi non dannosi, non esenta la 'ragionevole amministrazione della rete".

Le sub-clausole 1(a) e (b) dell'Articolo 8 del TiSA riproducono una sezione delle norme sull'"Open Internet" recentemente adottate dalla Federal Commination Commission [sic – probabile refuso e rectius Federal Communications Commission – n.d.t.], sezione concentrata sulla protezione contro il blocco degli utenti finali dall'accesso di contenuti e servizi e sull'utilizzo di dispositivi finali non dannosi (FCC, *In the Matter of Protecting and Promoting the Open Internet,* FCC 15-24, 26).

La neutralità della rete come principio protetto dalla legge si va rapidamente evolvendo in molte giurisdizioni e i suoi parametri completi devono ancora essere stabiliti. Sfortunatamente il TiSA non affronta efficacemente i problemi esistenti di neutralità della rete. Affronta significativamente soltanto le violazioni della neutralità più gravi (quelle relative al blocco dell'accesso ai contenuti) e

persino a tale riguardo esenta in generale la "ragionevole amministrazione della rete". Se tale approccio divenisse uno standard internazionale per l'accesso aperto neutrale incorporato come parametro internazionale, sarà un approccio non in grado di soddisfare la neutralità della rete di oggi, per non parlare di quella di domani. In realtà i quadri di neutralità della rete esistenti in Brasile, Canada e altrove adottano restrizioni più stringenti nei confronti dei fornitori di servizi che cerchino di bloccare l'accesso dei consumatori a servizi o contenuti a valle.

La sub-clausola 1(a) dell'Articolo 8 del TiSA è anche problematica perché si applica solo a situazioni in cui è bloccato l'accesso ad applicazioni o servizi. Non include situazioni in cui il traffico è degradato o discriminato ingiustificatamente in un senso economico. Tuttavia la maggioranza delle preoccupazioni sulla neutralità della rete è collegata a discriminazioni economiche o tecniche contro il traffico a valle.

La sub-clausola 2 dell'Articolo 8 del TiSA riconosce che le Parti dovrebbero "sforzarsi" di evitare "discriminazioni irragionevoli" da parte dei fornitori di servizi Internet (ISP) nella trasmissione di traffico legittimo in rete. Tuttavia non solo la "ragionevole discriminazione" è permessa (duplicando lo standard di "ragionevolezza" adottato dalla FCC che, come citato più sopra, è più permissivo di quelli adottati da altre giurisdizioni, quali Brasile e Canada) ma il TiSA non impone alcuna prescrizione riguardo alle azioni disciplinari riguardo a tale discriminazione. Lo "sforzo" non implica l'apparato di imposizione delle leggi dello stato e può ben precluderne l'utilizzo. A causa di questi limiti il quadro di accesso libero del TiSA lascia aperto un intero universo di attività discriminatorie e dannose per l'innovazione su cui i vettori di traffico possono far leva e che i regolatori hanno ritenuto reprensibili.

Se ciò divenisse lo standard internazionale per affrontare i danni all'accesso libero o alla neutralità della rete, lo farà in un modo che sarebbe miseramente carente.

Articolo 9 – Infrastruttura locale / Presenza locale

Articolo 9: [JP/CH/US propongono: Infrastruttura Locale][JP propone: e presenza locale][KR propone: 1]

1. [**KR propone:** L'Articolo 9 non si applica con riguardo ai fornitori di servizi o reti di telecomunicazioni pubblici].

1. [**CO/US propongono:** Nessuna Parte può richiedere a un fornitore di servizi, come condizione per fornire un servizio o per investire nel suo territorio, di:

a) utilizzare strutture informatiche localizzate nel territorio della Parte;

b) di utilizzare servizio di elaborazione o archiviazione informatica forniti dall'interno del territorio della Parte; o

c) altrimenti archiviare o elaborare dati nel suo territorio.]

[**CO propone:** Tuttavia nulla nel paragrafo 1 dovrebbe impedire a una Parte di subordinare il godimento o la prosecuzione del godimento di un vantaggio al rispetto della richiesta di utilizzare, creare o ampliare strutture informatiche nel proprio territorio, comprese quelle necessarie per elaborare o archiviare dati.]

[**KR propone:** Riguardo al paragrafo 1 [infrastrutture locali] la Corea ha riserve sull'accettazione dell'attuale formulazione, tenuto conto del nostro quadro di disciplina delle telecomunicazioni. La Corea è aperta alla discussione sulla limitazione o sulla definizione della portata dell'applicazione di questa norma.]

2. [**US propongono; KR/CO si oppongono:** Questo articolo si applicherà ai fornitori transnazionali di servizi finanziari solo nella misura in cui i servizi finanziari transnazionali sono coperti da impegni specifici di una Parte].

[**JP** vorrebbe fosse chiarito il significato del paragrafo 2.][**KR:** Riguardo al paragrafo 2 la Corea ritiene che

ciò possa essere affrontato nell'Allegato sui Servizi Finanziari. La Corea suggerisce la cancellazione di questo paragrafo e al tempo stesso appoggia la proposta svizzera/giapponese di escludere i servizi finanziari da questo allegato, come nell'Articolo III.X delle Norme Generali.]

3. [**KR si oppone; [JP propone:** Nessuna Parte dovrà][**CH propone:** Le Parti non dovrebbero][**JP/CH propongono:** richiedere] [**JP propone:** ai fornitori di servizi ICT [Information and Communication Technology – n.d.t.]][**CH propone:** ai fornitori di commercio elettronico] [**JP/CH propongono:** di utilizzare][**CH propone:** o stabilire qualsiasi][**JP/CH propongono:** infrastruttura locale come condizione per][**JP propone:** fornire][**CH propone:** la fornitura di][**JP/CH propongono:** servizi.]]

4. **[KR si oppone; [JP propone:** Nessuna Parte richiederà ai fornitori di servizi ICT di stabilire una presenza locale come condizione per la fornitura transnazionale di servizi.]]
[**JP** desidererebbe cancella il paragrafo 4 di questo Articolo se la presenza locale deve essere disciplinata nel testo centrale del TiSA.][**KR** ha riserve sull'articolo sulla Presenza Locale [paragrafo 4 dell'Articolo 9 proposto dal Giappone.]

5. [**KR si oppone; [JP propone:** Nessuna Parte dovrà][**CH propone:** Inoltre le Parti non dovrebbero][**JP/CH propongono:** dare priorità o concedere trattamenti speciali a][**JP propone:** propri fornitori di servizi][**CH propone:** fornitori nazionali di commercio elettronico][**JP/CH propongono:** nell'uso di infrastrutture locali,][o di risorse – n.d.t.] [**JP propone:** nazionali] [**CH propone:** terrestri][**JP/CH propongono:** di spettro][**JP propone:** ,] [**JP/CH propongono:** o satellitari]]

[**CO** vorrebbe escludere da questa norma le questioni collegate all'approvvigionamento governativo.]

La proposta di USA e Colombia sulla localizzazione dei dati afferma che "nessuna Parte può richiedere a un fornitore di servizi di utilizzare strutture informatiche territorialmente localizzate per l'elaborazione e l'archiviazione di dati come condizione di fornitura o investimento in tale paese." Questo obbligo si applica a tutti i fornitori di servizi (esistenti e futuri), comprese società nazionali private e imprese di proprietà statale. Le restrizioni si applicano a "fornire un servizio o investire nel suo territorio", il che è di vasta portata poiché si applica a tutti gli elementi diretti e indiretti della catena di fornitura di un servizio.

L'USTR [Rappresentante per il Commercio degli Stati Uniti – n.d.t.] da tempo considera ogni prescrizione di utilizzare infrastrutture locali di rete o server locali come barriere non tariffarie e restrizioni discriminatorio ai diritti del commercio, affermando che le prescrizioni di localizzazione sono strategie protezioniste del commercio che svantaggiano merci, servizi o proprietà intellettuali stranieri rispetto a beni nazionali. Gli USA ritengono anche che le prescrizioni di localizzazione indebolirebbero il vantaggio di servizi statunitensi su base 'cloud', poiché la maggior parte delle imprese, se non tutte, che utilizzano servizi su base 'cloud' ha attualmente sede negli Stati Uniti.

Prescrizioni generalizzate di server locali, senza alcuna esenzione, sono sproporzionate e possono avere un effetto deleterio sull'economia digitale. Ciò nonostante l'informatica via 'cloud' sta rapidamente conquistando popolarità tra i fornitori di servizi, il che fa sorgere domande importanti riguardo alla responsabilità dei fornitori di servizi. L'attuare quadro legislativo sulla riservatezza è lungi dall'essere ideale. Esistono leggi e regolamenti divergenti sulla riservatezza. La localizzazione dei dati spesso determina le leggi applicabili su come i dati sono elaborati e archiviati. La maggior parte delle imprese ICT statunitensi archivia i dati negli USA, il che rende le norme statunitensi applicabili alla conservazione, all'elaborazione e al trasferimento dei dati. Il livello inadeguato di protezione dei dati negli USA potrebbe essere considerato una barriera commerciale per le parti negoziatrici non statunitensi con leggi rigorose sulla riservatezza e sulla conservazione dei dati.

Gli Stati Uniti vogliono limitare l'applicazione di questo articolo ai fornitori di servizi finanziari transnazionali alla misura in cui i servizi finanziari transnazionali sono coperti da specifici impegni di una Parte. La Svizzera e il Giappone vogliono escludere i servizi finanziari dall'Allegato, e la Corea appoggia tale proposta. L'Articolo X.11 del capitolo del TiSA filtrato sui servizi finanziari disciplina il trasferimento transnazionale di informazioni [https://wikileaks.org/tisa-financial/]. Merita di essere notato che la bozza di "Legge sul Commercio Digitale" introdotta nel Senato USA nel dicembre del 2013, conferirebbe al Rappresentante del Commercio degli Stati Uniti un mandato vincolante per negoziati internazionali nell'area del commercio elettronico. Le norme sulla "localizzazione" dovrebbero essere bandite e norme sull'"interoperabilità" dell'elaborazione dei dati sarebbero onorate come principio fondamentale. Questa Legge ovviamente si applicherebbe anche ai negoziati sul capitolo corrispondente dell'accordo TTIP.

Giappone e Svizzera propongono che un governo non possa richiedere a un fornitore di servizi (di commercio elettronico o ICT) di utilizzare o creare qualsiasi infrastruttura locale come condizione per la prestazione di un servizio (con riferimento a tutti gli elementi, diretti e indiretti, della catena di prestazione di un servizio). Questa norma impedisce a un governo di richiedere che strutture informatiche, compresi i server, siano localizzate nel suo territorio.

Secondo il paragrafo 4 proposto dal Giappone una presenza locale non può essere resa "condizione" per la fornitura transnazionale di un servizio. Il Giappone vuole essere in grado di prestare servizi ICT senza essere richiesto di avere un ufficio fisico nei paesi TiSA. La norma inciderebbe solo su servizi che richiedono una qualche forma di approvazione e si applica a servizi che possono essere forniti nel paese solo da fornitori autorizzati o registrati o da operativi provvisti di licenza, quali le società che prestano servizi di contabilità, legali, sanitari, di ingegneria, ecc..

Il Giappone, tuttavia, vuole cancellare il paragrafo se il tema della presenza locale è affrontato nel testo centrale del TiSA.

Articolo 10 - Autenticazione Elettronica e Firme Elettroniche

Articolo 10: Autenticazione Elettronica e Firme Elettroniche

1. [**AU/CA/TW/CO/UE/IS/KR/MX/NO/PA/PE/TR/US propongono:** A eccezione di quanto diversamente disciplinato nella propria legge, una Parte non negherà la validità di una firma unicamente sulla base del fatto che tale firma ha forma elettronica.

[**JP** vorrebbe chiarire il significato di "a eccezione di quanto diversamente disciplinato nella propria legge" nel paragrafo 1].

2. [**AU/CA/TW/CO/UE/IS/JP/KR/MX/PE/TR/US propongono:** Nessuna Parte può adottare o mantenere misure per l'autenticazione elettronica che:

a) vietino alle parti di una transazione elettronica di decidere mutuamente i metodi appropriati di autenticazione per tale transazione; o
b) impediscano alle parti di avere l'opportunità di stabilire di fronte all'autorità giudiziaria o amministrativa che la loro transazione elettronica è conforme a ogni prescrizione legale quanto all'autenticazione.

3. [**AU/CA/TW/CO/UE/IS/JP/KR/MX/PE/TR/US propongono:** Nonostante il paragrafo 2 una Parte può richiedere che, per una particolare categoria di transazioni, il metodo di autenticazione soddisfi certi parametri prestazionali o sia certificato da un'autorità accreditata in conformità con la legge della Parte.]

Questa norma mira a minimizzare le restrizioni all'uso delle firme elettroniche. E' basata sulla proposta USA datata 25 aprile 2014. Conseguentemente un governo non può negare la validità legale di una firma solo perché elettronica. Anche se la norma appare rigorosa, resta subordinata alla legge nazionale. La legge nazionale può impedire o limitare il riconoscimento legale della validità delle firme elettroniche.

Sulla base di questa norma ben sostenuta un governo non può introdurre o mantenere prescrizioni per l'autenticazione che impediscano alle parti di una transazione elettronica di decidere autonomamente quale è il modo migliore per autenticare la transazione. Un governo non può nemmeno impedire a parti di una transazione elettronica di dimostrare a organi giudiziari o amministrativi che la loro transazione rispetta la legge per quanto riguarda l'autenticazione.

Il paragrafo 3 consente che parametri prestazionali siano fissati per l'autenticazione e consente la richiesta di certificazione da parte di un'autorità accreditata, ma solo quando una misura sia sostanzialmente correlata a conseguire un "obiettivo governativo legittimo". Un governo può ancora richiedere che una "particolare categoria di transazioni" soddisfi certi parametri prestazionali o sia certificata da un'autorità accreditata nel rispetto della legge nazionale. Non ci sono indicazioni di quali possano essere tali categorie e perciò non ci sono limiti alla loro portata e al loro numero.

Articolo 11 – Diritti Doganali sulle Consegne Elettroniche

Articolo 11: [AU/CO/UE/IS/NO/PE/CH/TW propongono: Diritti Doganali sulle Consegne Elettroniche

[**UE/NO propongono:** Le Parti concordano che una consegna trasmetta attraverso mezzi elettronici non sia assoggettata a diritti doganali, [**TW si oppone:** imposte o gravami].[**CO/CR/JP/PE propongono:** Nessuna Parte può imporre diritti doganali [**TW si oppone:** imposte o gravami] sulle trasmissioni elettroniche.]

2. Per maggiore chiarezza, il paragrafo 1 non impedisce a una Parte di imporre imposte nazionali o altri gravami interni sulle [**UE/NO propongono:** consegne effettuate attraverso mezzi elettronici][**CO/MX/PE propongono:** trasmissioni elettroniche] a condizione che tali imposte o gravami siano imposti in modo coerente con questo Accordo.]

Anche se la norma prevede che i servizi resi mediante trasmissione elettronica non siano soggetti a diritti, imposte o gravami doganali, la norma non impedisce a un governo di imporre imposte o altri gravami interni per una consegna trasmessa attraverso mezzi elettronici a condizione che tali imposte o gravami siano imposti in modo coerente con l'Accordo.

Se una consegna trasmessa attraverso mezzi elettronici è esentata da diritti doganali, andranno persi i diritti doganali all'importazione. I paesi, specialmente quelli in via di sviluppo, in cui i diritti doganali svolgono un ruolo considerevole nel bilancio nazionale dovrebbero considerare con attenzione la difficoltà di sostituire le entrate perse prima di bloccarsi in uno status permanente di esenzione dai dazi nella consegna attraverso mezzi elettronici.

Articolo 12 – Cooperazione Internazionale

Articolo 12: [JP/CH propongono: Cooperazione Internazionale]

1. [**CO/JP/NO propongono:** Ciascuna Parte si sforzerà di collaborare con altre Parti per accrescere globalmente il livello di alfabetismo digitale e di ridurre il "divario digitale".]

2. [**CO/CH propongono:** Le Parti scambieranno [**CO propone:** per quanto possibile] informazioni nell'area

del commercio elettronico e dei servizi di telecomunicazione. Ciò può comprendere, inter alia, informazioni su:

a) sviluppi e ricerche tecnologiche nell'area del commercio elettronico e dei Servizi di telecomunicazione;
b) aspetti tecnici e commerciali dell'offerta di commercio elettronico e di Servizi di telecomunicazione in tutte le modalità di fornitura;
c) possibilità disponibili di scambio di commercio elettronico e di tecnologia collegata alle telecomunicazioni; e
d) leggi e regolamenti applicabili, procedure legislative e sviluppi legislativi recenti; parametri tecnici applicabili.]

3. [**CO/NO/CH propongono:** le Parti scambieranno idee sugli sviluppi relativi al commercio elettronico e ai Servizi di telecomunicazione a livello internazionale.]

4. [**CH propone: Promozione**

Le Parti affermano la loro intenzione di:

a) promuovere queste norme al fine di contribuire all'espansione e alla diffusione del commercio elettronico e dei servizi di telecomunicazione;

b) collaborare e cooperare in forum internazionali per accrescere il livello di alfabetismo digitale e di ridurre il divario digitale globale;

c) cooperare con paesi terzi nell'ottica di promuovere la capacità normativa nazionale e di contribuire alla diffusione del commercio elettronico e dei Servizi di telecomunicazione, che sono strumenti potenti per la promozione dello sviluppo economico.]

L'alfabetismo digitale può essere definito come la capacità di utilizzare tecnologia digitale, strumenti o reti di comunicazione per localizzare, valutare, utilizzare e creare informazioni. L'alfabetismo digitale dipende da modalità digitali di comunicazione e agevola la collaborazione e la condivisione del sapere. D'altro canto il divario digitale è un concetto complesso e dinamico e descrive le differenze di accesso all'ICT. Tuttavia non esiste un divario unico, bensì molteplici divari e perciò ci sono numerosi modi per misurare il divario digitale.

Anche se il commercio elettronico ha aperto nuove opportunità economiche globali, è molto probabile che tali sviluppi possano ampliare il divario digitale e i paesi in via di sviluppo possono restare indietro e perdere nella gara. Perciò il coordinamento e lo scambio di informazione a livello internazionale divengono importanti. Questa norma promuove la cooperazione e lo scambio di informazioni tra i governi ma non impone alcun obbligo.

Articolo 14

[US propongono: Nulla nella Sezione III (Commercio Elettronico) sarà interpretato come un divieto a qualsiasi Parte di intraprendere qualsiasi iniziativa che consideri necessaria per la protezione dei propri interessi essenziali di sicurezza.]

[**CO/JP** desidererebbero chiarire il significato di "interessi essenziali di sicurezza" nel paragrafo 1 di questo articolo.]

[**KR:** La Corea vorrebbe una maggiore discussione su che cosa si intenda per "interessi essenziali di sicurezza" in questo articolo.]

Questa eccezione proposta dagli Stati Uniti protegge il diritto di un governo di assumere qualsiasi iniziativa ritenga necessaria per proteggere i propri essenziali interessi di sicurezza. Questa norma non prevede alcuna limitazione o riserva. Nell'applicare queste eccezioni i governi dovrebbero soppesare il danno all'interesse pubblico.

L'eccezione relativa alla sicurezza nazionale è auto-referenziale. Gli Stati Uniti si sono rifiutati di sottoporsi a qualsiasi disputa che abbia contestato il loro utilizzo di una norma simile, ma più debole, nell'ambito del GATT e della WTO.

Articolo 15 – Definizioni

Ai fini di questo Allegato:

[**AU/CO propongono: Autenticazione** significa la procedura o l'atto di stabilire l'identità di una Parte in una transazione o comunicazione elettronica o di assicurare l'integrità di una comunicazione elettronica;]

[**CO propone: Commercio elettronico** significa ogni attività economica o transazione commerciale trans-nazionale condotta utilizzando mezzi elettronici, compresi, tra gli altri, contratti di servizi di distribuzione, di lavori di costruzione, di servizi di consulenza, di servizi di ingegneria e di servizi commerciali.]

[**UE/TR propongono: Firma elettronica** significa dati in forma elettronica che sono allegati o logicamente associati ad altri dati elettronici e soddisfa i seguenti requisiti:

i. è utilizzata da una persona per accettare i dati elettronici cui si riferiscono;
ii. è collegata ai dati elettronici cui si riferisce in modo tale che qualsiasi alterazione successiva dei dati sia individuabile.]

[**AU/CO/NZ propongono: Informazioni personali** significa qualsiasi informazione, inclusi dati, relativa a una persona fisica individuata o individuabile].

[I proponenti si consulteranno sulla definizione di 'informazioni personali'].

[AU propone: Messaggi elettronici commerciali non richiesti significa messaggi elettronici che sono trasmessi a fini commerciali o di marketing a un indirizzo elettronico senza il consenso del destinatario o contro l'esplicito rifiuto del destinatario, utilizzando un fornitore di servizi d'accesso a Internet e, nella misura prevista dalle leggi e dai regolamenti nazionali di ciascuna Parte, altri servizi di telecomunicazione.]

Autenticazione: Anche se la nozione di autenticazione adempie funzioni diverse nei sistemi legali, è generalmente ritenuta riferirsi alla genuinità di un documento o di un flusso, che riferisce l'originalità del documento e conferma le informazioni contenute nella forma in cui sono state registrate e senza alcuna alterazione. La diversa definizione legale dell'autenticazione in vari sistemi legali può causare confusione su particolari procedure o prescrizioni di forma. La definizione proposta da Australia e Colombia è la stessa definizione contenuta nell'Accordo di Libero Scambio Australia-USA [Articolo 16.8, Australia-USA FTA, https://ustr.gov/sites/default/uploads/agreements/fta/australia/asset_upload_file508_5156.pdf]

Firma elettronica: La definizione proposta imita la definizione di "firma elettronica avanzata" prevista nella Direttiva [probabilmente la Direttiva Europea sulla Protezione dei Dati, v. oltre – n.d.t.]. Andrebbe notato che con lo sviluppo di nuove forme tecnologiche, prevedere una forma specifica di firma digitale nella normativa non è desiderabile. Una definizione generale di 'firma elettronica' aiuterà i governi a stabilirne l'utilizzo per ciascuna modalità di firma e a coordinare l'autenticità con altri partner.

Dati personali: Il modo in cui l'espressione "dati personali" è definita determina l'applicabilità e la portata delle leggi sulla riservatezza. La definizione proposta da Australia, Colombia e Nuova

Zelanda imita la definizione di dati personali contenuta nella Direttiva Europea sulla Protezione dei Dati: “informazioni relative a una persona fisica identificata o identificabile”. Considerata la molteplicità delle definizioni concorrenti nella legislazione statunitense questa norma può risultare estensiva per gli Stati Uniti.

I trasferimenti transnazionali di dati dipendono in larga misura dal coordinamento tra sistemi legali; la divergenza tra le definizioni di ‘dati personali’ ha molte probabilità di creare problemi per la protezione della riservatezza.

Nuove Previsioni Applicabili a Tutti i Servizi

[L’inclusione in questo documento di lavoro degli articoli seguenti della proposta statunitense per la Parte III del testo centrale del TiSA è intesa ad agevolare la discussione e non pregiudica l’inclusione e l’adeguamento finale di tali articoli nel testo centrale del TiSA o in un Allegato.]

L’analisi della proposta statunitense filtrata in precedenza [Trade in Services Agreement TiSA Proposal New Provisions Applicable to All Services Aprile 25, 2014] disponibile qui: http://www.world-psi.org/sites/default/files/documents/research/briefing_on_tisa_e-commerce_final.pdf

Originale: https://wikileaks.org/tisa/ecommerce/05-2015/analysis/page-1.html