

# Cybersecurity e privacy tra norme europee e prospettive internazionali: il caso dell'informazione economico-finanziaria

Elisabetta Zuanelli

Presidente CReSEC/Università degli Studi di Roma «Tor Vergata»

Coordinatore Partenariato «Piano nazionale di formazione in cybersecurity, cyberthreat, privacy»

[www.cybersecurityprivacy.it](http://www.cybersecurityprivacy.it)

# Tre quesiti

- Sovranità normativa nell'economia digitale: tra norme nazionali, europee e internazionali
- Le responsabilità istituzionali europee
- Discrasia normativa tra NIS e GDPR

# Impatti e prospettive delle regole e degli accordi internazionali sull'economia digitale

Le iniziative :

- il **DSM (Digital Single Market)**: 3 pilastri 16 azioni, 415 miliardi di euro l'anno di crescita stimata
- Il **TTIP (Transatlantic Trade and Investment Partnership)**: 800 milioni di consumatori
- Il **TiSA: Trade in Services Agreement**
- Il **CETA: Comprehensive Economic and Trade Agreement**



A Digital Single Market Strategy for Europe  
{SWD(2015) 100 final} Brussels, 6.5.2015 COM(2015) 192 final  
(15 July 2014) Jean-Claude Juncker

Priority n°2: A Connected Digital Single Market

- "dovremo avere il coraggio di abbattere i '*silo*' nazionali nella **regolazione delle telecomunicazioni**, nel **copyright** e nella legislazione di **protezione dei dati**, nella gestione delle **bande radio** e nell'applicazione della **normativa sulla concorrenza...**"
- "per raggiungere lo scopo, entro i primi sei mesi del mio mandato, intendo compiere **ambiziosi passi legislativi verso un mercato unico digitale connesso**, in particolare concludendo rapidamente le negoziazioni su regole europee comuni di protezione dei dati..."

## Ambiente regolatorio per piattaforme e intermediari

**Alcune piattaforme possono controllare l'accesso ai mercati on-line e possono esercitare un'influenza notevole su come i vari attori del mercato sono remunerati.** Ciò ha portato a una serie di preoccupazioni sul potere di mercato in crescita di alcune piattaforme. Queste includono la **mancaanza di trasparenza sul modo di utilizzare le informazioni che acquisiscono, il loro forte potere contrattuale rispetto a quello dei loro clienti,...**(in particolare per le piccole e medie imprese ), la **promozione dei propri servizi a scapito dei concorrenti e le politiche dei prezzi non trasparenti**, o restrizioni sulle condizioni di prezzo e di vendita. Alcune piattaforme si sono evolute **in competizione in molti settori dell'economia e il modo in cui usano il loro potere di mercato solleva una serie di questioni** che meritano un'ulteriore analisi oltre l'**applicazione del diritto della concorrenza** in casi specifici...

# ...platforms

*The Commission will launch before the end of 2015 a comprehensive assessment of the role of platforms, including in the sharing economy, and of online intermediaries, which will cover issues such as (i) **transparency** e.g. in search results (involving paid for links and/or advertisement), (ii) **platforms' usage of the information they collect**, (iii) relations between platforms and suppliers, (iv) **constraints on the ability of individuals and businesses to move from one platform to another** and will analyse, (v) how best to **tackle illegal content on the Internet**.*

The Commission will propose in 2016 a European 'Free flow of data' initiative **that tackles restrictions on the free movement of data for reasons other than the protection of personal data within the EU and unjustified restrictions on the location of data for storage or processing purposes.** It will address the emerging issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data. It will encourage access to public data to help drive innovation. **The Commission will launch a European Cloud initiative including cloud services certification, contracts, switching of cloud services providers and a research open science cloud.**

# Il TTIP: Transatlantic Trade and Investment Partnership: servizi finanziari (negoziati avviati nel 2013)

Il TTIP del luglio 2015 (All. b, Sezione 3, Computer services e Sezione 6, liberalizzazione dei servizi finanziari), apre **due fronti essenziali del dibattito**:

- servizi bancari, finanziari e **assicurativi** e **nuovi servizi** quali “la fornitura e il trasferimento di informazione finanziaria, la processazione dei dati finanziari e il software connesso”
- (Art. 5-33) “**l’autorizzazione al fornitore di un servizio finanziario di trasferire l’informazione finanziaria in formato elettronico o in altra forma, dentro e fuori del proprio territorio** per la processazione dei dati ove tale processazione sia necessaria nel corso ordinario del business del fornitore di servizi finanziari”



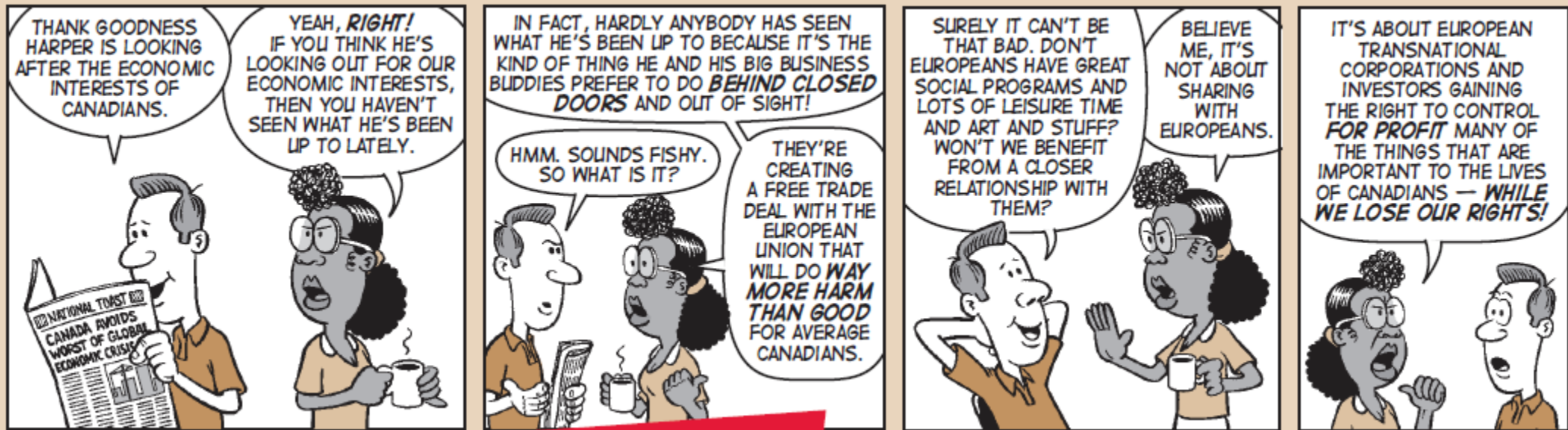
# TiSA: Trade in Services Agreement:

## liberalizzazione dei flussi di dati

TiSA, allegato (bozza Art. X.11) intitolato al ‘Trasferimento dei dati **evitando la localizzazione degli stessi**’: la stessa logica di liberalizzazione della processazione e del trasferimento dei dati, contro la previsione europea di mantenere la protezione dei dati economico-finanziari stessi almeno all’interno del territorio

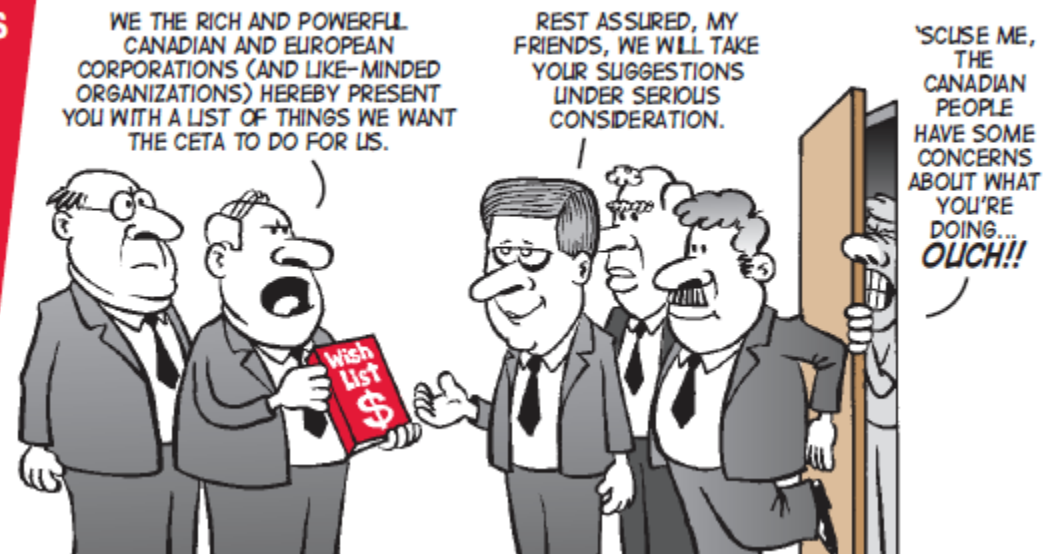
# II CETA: Comprehensive Economic and Trade Agreement

- CHAPTER FIFTEEN - TELECOMMUNICATIONS
- In this Comprehensive Economic and Trade Agreement chapter the EU and Canada commit to giving each other's businesses fair and **equal access to public telecommunications networks and services**. It includes **rules to ensure competition in the telecommunications market**. And it confirms customers' right to:
  - keep their number when switching providers and
  - receive telecommunications services in remote areas



**H**ey Canada, heard of the CETA yet? No? It's not surprising! Once again, our federal and provincial government and business leaders are negotiating a "free trade" deal behind the backs of Canadians. This time, it's called the Canada-European Union Comprehensive Economic and Trade Agreement, or CETA for short. It will change the face of Canada as we know it, and Harper wants to sign it in a hurry — *before anyone has a chance to debate it!*

Trade with Europe would be a good idea if it meant more good jobs and better social services. But like all "free trade" agreements, the CETA is not about that. It's about boosting corporate rights, lowering environmental standards, and weakening public services. As currently



# Liberalizzazione dei flussi di dati: norme generali sulla protezione dei dati e sicurezza?

**Non esistono norme europee né nazionali aggiornate sulla protezione dei dati di soggetti giuridici (Direttiva 95/46/EC, Regulation (EC) n. 45/2001 EDPS, Direttiva 2002/58/EC, CFDecision 2008/977/JHA)**

Il nuovo regolamento sulla *privacy* **esclude i soggetti giuridici**

**L'anonimazione di dati personali non elimina il rischio di esternazioni** e uso a scopo di mercato dei dati stessi, con implicazioni lecite e illecite

Il tema della 'protezione dei dati' non coincide con la *privacy* ma la ricomprende, include la cybersecurity, chiama in causa **diverse tipologie di soggetti addetti nei diversi settori**: intermediatori finanziari, controllori, certificatori, gestori di informazioni economico- finanziarie sensibili e di sistema in genere: statistiche, simulazioni, previsioni. I dati si acquisiscono, si elaborano, si correlano, si vendono, si hackerano: il **mercato e i rischi della *data economy***

# Perché la protezione dei dati è rilevante per la regolamentazione dei servizi finanziari (EDPS European data protection supervisor)

L'obiettivo della regolamentazione dei servizi finanziari in Europa è quello di garantire la stabilità finanziaria, un mercato unico efficiente per i servizi finanziari, l'integrità del mercato e la fiducia.

Le misure in questo settore comprendono requisiti del capitale bancario e norme in materia di derivati, assicurazioni, titoli e fondi di investimento. infrastrutture dei mercati finanziari, servizi finanziari al dettaglio e sistemi di pagamento.

Dall'inizio della crisi finanziaria nel 2008 più di 40 nuove leggi sono state proposte, molte scaturite da impegni assunti dal G20, la maggior parte delle quali sono state adottate.

Questo ampio corpo di regolamento prevede una stretta supervisione del comportamento degli operatori e degli investitori nei mercati finanziari, attraverso maggiori poteri per le autorità di vigilanza, la trasparenza per tutti gli operatori di mercato, il controllo del rischio e la protezione dei consumatori, investitori e contribuenti contro le attività rischiose.

Altre misure, come le direttive in materia di riciclaggio di denaro e il finanziamento del terrorismo, e il regolamento sul regolamento finanziario applicabile al bilancio annuale dell'UE, impongono obblighi a carico delle istituzioni finanziarie.

La maggior parte di queste misure riguardano le azioni delle persone giuridiche.

Molte però, come quelle che riguardano la **sorveglianza, la tenuta dei registri e la segnalazione, lo scambio di informazioni, i poteri delle autorità competenti e le sanzioni per la violazione delle norme applicabili**, comportano il trattamento dei dati personali, cioè **i dati relativi a persone fisiche direttamente o indirettamente identificabili**.

Alcune misure potenzialmente interferiscono anche con il diritto alla *privacy*.

Fase 1: **identificare** le informazioni personali da elaborare

Fase 2: **valutare** se l'elaborazione delle informazioni interferisce con il diritto alla *privacy*

Fase 3: **definire** lo scopo del trattamento

Fase 4: **stabilire una base giuridica** per l'elaborazione dei dati

Fase 5: **stimare e giustificare** un periodo di conservazione adeguato

Fase 6: identificare quali parti all'interno dell'UE **possono avere accesso** all'informazione personale

Fase 7: creare una **base giuridica corretta** per qualsiasi trasferimento di dati personali al di fuori l'UE

Fase 8: Fornire **adeguate** garanzie di diritti di protezione dei dati degli individui

Fase 9: considerare le **misure di sicurezza dei dati appropriate**

# II TiSA: Trade in Services Agreement

**Evoluzione del WTO/GATS (General Agreement in Trade Services)**

**Definizione 'geografica' di fornitura di servizi:**

- (a) from the territory of one Member into the territory of any other Member;
- (b) in the territory of one Member to the service consumer of any other Member;
- (c) by a service supplier of one Member, through commercial presence in the territory of any other Member;
- (d) by a service supplier of one Member, through presence of natural persons of a Member in the territory of any other Member.



# I settori critici e le disposizioni istituzionali nel TiSA : la sovranità economico-finanziaria?

(Ecorys draft report 2014 e TiSA , Allegato 1B General Agreement on trade in services)

- Problematicità dei settori: Servizi finanziari e telecomunicazioni, ICT, *ecommerce* (Ecorys)
- *Institutional provisions* ( Parte V Annex: Article XXIII e XXIV e Allegati dell'Allegato su **servizi finanziari e digitale**):

**Dispute Settlement and Enforcement:** ricorso al DSU (*dispute settlement understanding*) e intervento del DSB (*dispute settlement body*)

**Istituzione del Council for Trade in Services** (Presidente e organismi sussidiari)

# I vantaggi del TiSA per la liberalizzazione dei servizi finanziari

- **migliorare l'accesso dei paesi al capitale internazionale**

- ☐ **abbassare i prezzi per i consumatori**

- ☐ **aiutare le aziende nazionali in difficoltà a ricapitalizzarsi**

- ☐ **incoraggiare il trasferimento tecnologico**

**se non regolati rischio di instabilità**

Le tecnologie nel mercato borsistico: l'Internet sottomarino e il *matching* dei dati

- **ruolo particolare nel commercio elettronico** di valuta estera interpretato da tre dei più grandi centri finanziari : Londra, New York e Tokyo
- in queste città **sono localizzati i server di corrispondenza di Electronic Broking Services ( EBS ) e Thomson Reuters**, le principali piattaforme di intermediazione elettronica e il commercio a partire dai primi 1990s
- ne consegue che la connessione di un paese nel Regno Unito (per Londra ), Stati Uniti (per New York) o in Giappone ( per Tokyo ) attraverso **un cavo sottomarino a fibre ottiche riduce i tempi di latenza e aumenta la larghezza di banda**
- in un mondo in cui **le esigenze di elaborazione dati crescono in modo esponenziale** e conti di trading ad alta frequenza per una quota in rapida crescita di FX trading, **sia larghezza di banda e il tempo di latenza** sono di fondamentale importanza

## UN Stiglitz Commission

“The framework for financial market liberalization under the Financial Services Agreement of the General Agreement on Trade in Services (GATS) under the WTO and, even more, similar provisions in bilateral trade agreements may restrict the ability of governments to change the regulatory structure in ways which support financial stability, economic growth, and the welfare of vulnerable consumers and investors.”

*Report of Commission of Experts, 2009*

## UNCTAD (United Nations Conference on Trade and Development) Trade and Development Report

“The General Agreement on Trade in Services (GATS) of the World Trade Organization (WTO), many bilateral trade agreements and bilateral investment treaties (BITs) include provisions relating to payments, transfers and financial services that may severely limit not only the application of capital controls, but also other measures aimed at re-regulating or restructuring financial systems.”

*Chapter 4, p. 100-103, UNTDR, 2011*

# I rischi

Public Citizen's Global Trade Watch

“Trade in Services Agreement: The Dangers of Liberalizing Services”

Geneva, Switzerland, 17 October 2014

- regole d'accesso al mercato che **impediscono di bandire** derivati tossici, limiti di grandezza per le entità in gioco, misure protettive nel rapporto depositi/investimenti
- **transfer rules** che proibiscono restrizioni sui flussi di capitali nei settori impegnati
- controlli di capitale **che consentono flussi «hot money» e asset bubbles**
- la Commissione europea aveva rilevato nel 2010 **conflitti potenziali con la Financial Transactions Tax**
- le eccezioni sono ambigue e di fatto **non consentono spazi di *policy* specifiche**

# Temi e problemi: *data economy* e sovranità economico-finanziaria

Come proteggere i dati? *Insider malicious* e *cybersecurity*

- **TiSA verrebbe a contraddire** sforzi per incoraggiare una robusta regolazione finanziaria atta a evitare crisi future (G20, Basilea, ecc.)
- **Impossibilità di interventi nazionali per la stabilità economica** e la difesa dei consumatori e delle PMI (perdita della sovranità economico-finanziaria)
- **Perdita di ruolo della Commissione europea e del Parlamento europeo:** le Direzioni Trade della UE stanno trattando senza consultazione dei sistemi Paese e non sembrano interfacciate con le DDGG di competenza ovvero la DG servizi finanziari e la DG Connect
- Qual è oggi e **quale sarebbe nel futuro il ruolo della politica e delle istituzioni nazionali** se nella *deregulation* non è previsto uno spazio di *policy* per la regolazione finanziaria e per l'economia nazionale in genere?
- **Istituzione di un governo sovranazionale, sovraeuropeo, globale dell'economia** con regole non più nazionali

# Le Direzioni europee

## La Communications Networks, Content and Technology (DG Connect)

The Directorate-General for Communications Networks, Content and Technology is the Commission department responsible to develop a **digital single market** to generate smart, sustainable and inclusive growth in Europe



# Le Direzioni europee 2

## Directorate-General FISMA

### Financial Stability, Financial Services and Capital Markets Union

The Directorate-General for Financial Stability, Financial Services and Capital Markets Union is the Commission department responsible for EU policy on banking and finance

# Le Direzioni europee 3

## Directorate-General DIGIT Informatics

The Directorate-General for Informatics is the Commission department responsible for providing digital services that support other Commission departments and EU institutions in their daily work and that help public administrations in EU member countries work better together

# Direzioni europee 4

## Directorate-General RTD Research and Innovation

This Commission department is responsible for EU policy on research, science and innovation, with a view to help create growth and jobs and tackle our biggest societal challenges

# Direzioni europee 5

Directorate-General TRADE

Trade

This Commission department is responsible for EU policy **on trade** with countries beyond the EU's borders

# Direttiva NIS, GDPR, Eprivacy, e Directive. Privacy shield

Come concorrono i diversi soggetti e a chi le responsabilità:

- Le direzioni generali
- Il gruppo dei 29
- Organismi vari
- Il garante europeo, ecc.

# Le norme

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)

DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

*Il Privacy shield*

# Direttiva NIS/Discrasie?

## **Articolo 2 Trattamento di dati personali**

- 1. Il trattamento di dati personali ai sensi della presente direttiva è effettuato ai sensi della direttiva 95/46/CE.
- 2. Il trattamento di dati personali da parte di istituzioni e organismi dell'Unione ai sensi della presente direttiva è effettuato a norma del regolamento (CE) n. 45/2001.

# I Considerando 72 e 73 della Direttiva NIS

- (72) Lo scambio di informazioni sui rischi e sugli incidenti all'interno del gruppo di cooperazione e della rete di CSIRT e il rispetto degli obblighi di notifica degli incidenti alle autorità nazionali competenti o ai CSIRT potrebbero richiedere il trattamento di dati personali. Tale trattamento **dovrebbe essere conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio (1) e al regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio (2)**. Nell'applicazione della presente direttiva si applica, per quanto di ragione, il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio (3).
- (73) Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e **ha espresso un parere il 14 giugno 2013 (4)**



# Problematicità 1

- Correlazione NIS con GDPR (cessazione delle norme pregresse e *eprivacy*)

Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso un parere il 14 giugno 2013 (4).

Il trattamento di dati personali ai sensi della presente direttiva è effettuato ai sensi della direttiva 95/46/CE. 2. Il trattamento di dati personali da parte di istituzioni e organismi dell'Unione ai sensi della presente direttiva è effettuato a norma del regolamento (CE) n. 45/2001.

# Problematicità 2

- Cybersecurity e protezione dei dati: come applicarli al sistema AAPP, PMI, Enti locali, ecc.
- *Compliance vs security*
- Interessi economici vs interessi sociali
- Crescita, concorrenza, monopoli

E' tutto. Grazie!