

Le problematiche in tema di privacy e data protection

Avv. Daniele Vecchi

Roma, 10 novembre 2014

Dal FATCA al CRS

Il **Foreign Account Tax Compliance Act (FATCA)** è una legge federale degli Stati Uniti, approvata il 18.3. 2010, che richiede

- alle società e ai cittadini statunitensi, inclusi quelli che vivono all'estero, di trasmettere alcuni dati relativi alla loro situazione finanziaria, alle autorità fiscali US, e
- alle istituzioni finanziarie, anche straniere, di trasmettere al US Internal Revenue Service (IRS) dati sulla situazione finanziaria dei loro clienti di nazionalità statunitense.

Il Codice della Privacy: il problema

La privacy introduce limiti nella raccolta e nel trattamento dei dati

La necessità di rispettare leggi estere (le sorprendenti leggi “over-sea”) **non** scrimina



L'esempio eclatante:
Il caso Swift

Il Caso Swift

SWIFT - Society for Worldwide Interbank Financial Telecommunication, con sede legale in Belgio e sede operativa negli US, aveva trasmesso negli US dati sulle transazioni finanziarie effettuate per conto delle banche clienti, come richiesto «*sub poena*» ai sensi del Patriot Act.

Diverse Autorità Garanti Europee hanno affermato che la trasmissione di informazioni contenute nelle transazioni finanziarie richiesta da parte del Governo US costituisce violazione della normativa UE e nazionale a tutela dei dati personali.

Le leggi "overseas"

- Il «*whistleblowing*». La **US Sarbanes-Oxley Act (SOX)**: obbliga le società quotate negli US, le loro controllate con sede nell'UE e le società straniere negoziate sui mercati regolamentati US ad adottare «*procedure per la ricezione, l'archiviazione e il trattamento di denunce riguardanti la tenuta della contabilità, i controlli contabili interni e la revisione contabile, nonché per la presentazione in via confidenziale o anche anonima di segnalazioni da parte di dipendenti in merito a pratiche contabili o di revisione censurabili*» (art. 301).

Si tratta di un meccanismo di raccolta e trattamento dei dati dei lavoratori potenzialmente molto invasivo, e che ha formato oggetto di accese discussioni.

Le leggi "overseas"

- **Public Company Accounting Oversight Board (PCAOB):** le Autorità UE hanno posto notevoli restrizioni alla trasmissione da parte delle società di revisione Europee della documentazione relativa agli incarichi di revisione contabile al PCAOB negli USA, così come prevista dall'art. 106 del SOX, ritenendo la giurisdizione USA non idonea a fornire un livello adeguato di protezione dei dati;
- **Il trasferimento dei dati dei passeggeri aerei alle Autorità USA:** la messa a disposizione a lungo termine delle Autorità di sicurezza USA dei dati dei passeggeri dei voli per e dagli USA, la cui mancanza può portare a pesanti sanzioni e/o perdita dei diritti di atterraggio, è stato ritenuto violare il diritto fondamentale alla protezione dei dati personali degli interessati.
- Le varie (numerose) **investigazioni di autorità amministrative US** (Dipartimento di Stato, Autorità Antitrust, Ministro della Sanità, ma anche PCAOB, Autorità FCPC) configurano serie problematiche privacy.

Applicare il FATCA

- Fatca è una «normativa oversee»?

Assolutamente sì. The Economist (28 giugno 2014) ha definito FATCA "*extraterritoriality stunning even by Washington's standards*"

- Fatca richiede il trattamento di dati personali dei propri clienti, da parte delle istituzioni finanziarie?

Assolutamente sì. Oltre che dati comuni possono essere trattati anche dati sensibili.

- Tale trattamento deve conformarsi alle normative sul trattamento dei dati localmente vigenti?

Assolutamente sì

Il Parere dell'Article 29 Working Party

Su richiesta della DG TAXUD (Direzione Generale Tasse e Dogane della Commissione Europea), il WP ha emanato il 21.6.2012 un parere sulla compatibilità fra il FATCA e la normativa comunitaria in materia di privacy ed ha espresso le sue perplessità

A fronte di una lettera della DG TAXUD, il 1.10.12 il WP trasmetteva i chiarimenti richiesti e confermava le sue preoccupazioni.

II Parere dell'Article 29 Working Party

- In the absence of a lawful basis to legitimise the processing required, WP29 does not see how compliance of FATCA and the Directive could be simultaneously achieved.
- Currently there is no legal basis within EU or national law of a Member State to ensure lawful processing of the data within the scope of FATCA. If this remains the case on the entry into force of FATCA, EU/EEA data protection authorities (DPAs) may consider prohibiting the data processing in question.
- It was originally intended that the above measures would be contained within agreements between the FFIs and the IRS. (...) The original intention was to incentivise compliance with a number of sanctions for non-compliance on any FFI that fails to enter into an agreement with the IRS and on any “recalcitrant” accountholder.

Il Parere dell'Article 29 Working Party

- Under the (nuovo ed alternativo) Intergovernmental Approach, «Signatories to the alternative approach would be committed to creating new legislation or amending existing legislation that would introduce a legal obligation for FFIs to enhance their existing due diligence procedures and share the relevant information with their own tax authority”
- The Intergovernmental Approach would reduce the administrative burden on FFIs by removing the requirement for them to:
 - enter into an agreement with the IRS;
 - report information on US accounts directly to the IRS;
 - terminate the account of a recalcitrant account holder; and
 - withhold on passthru payments to recalcitrant account holders or to FFIs in FATCA partner countries”.

Applicare il FATCA

I governi di Stati Uniti da un lato e Francia, Germania, Italia, Spagna e Regno Unito dall'altro hanno sottoscritto una lettera di intenti e manifestato l'intenzione di collaborare per implementazione di FATCA, recependo la norma nei propri ordinamenti e rendendo obbligatorio l'adeguamento da parte degli operatori, superando così i vincoli di applicabilità connessi alla normativa in materia di trattamento dei dati personali e al segreto bancario, ove presenti.

Per i paesi sottoscrittori dell'IGA gli USA, oltre ad uno slittamento della scadenza e all'impegno di reciprocità nello scambio dei dati dei potenziali evasori, hanno introdotto serie di semplificazioni, fra cui la possibilità di sfruttare le procedure di antiriciclaggio in vigore per l'identificazione della clientela.

Applicare il FATCA

L'Italia ha firmato l'IGA - Intergovernmental Agreements l'10 gennaio 2014.

Il Consiglio dei Ministri del 30.6.2014 ha approvato un disegno di legge di ratifica ed esecuzione dell'accordo IGA, presentato alla Camera il 28 luglio 2014, iscritto con il numero C. 2577 e attualmente (dal 22.10) in esame in commissione

Il 2 luglio 2014, il Dipartimento delle Finanze ha emanato bozza di decreto attuativo della legge di ratifica.

Tutto risolto, dunque?

Il parere del WP del giugno 2012 ammonisce che: «however Member States may choose to recognise FATCA and/or implement it, they should take care to ensure that the law governing this mechanism has sufficient quality and foreseeability with regard to data protection safeguards contained within it. (European Court of Human Rights - Leander vs Sweden, 26 March 1987, para. 51 and Rotaru, 4 May 2000, para. 52).

Member States should also ensure that any law governing the processing and transfer – and any (bilateral) agreement derived from it should take into account the obligations in the Directive and, where appropriate and necessary, engage with the relevant data protection authority to ensure that the best possible data protection safeguards are in place».

Il recepimento dell'accordo intergovernativo

- Né l'Accordo Intergovernativo, né la legge di ratifica, né il Decreto Attuativo del Ministero delle Finanze, fanno alcun riferimento alla normativa Europea o Italiana in materia di privacy, né introducono alcun meccanismo di tutela.
- Soltanto in sede di «analisi tecnico normativa» della norma di ratifica viene previsto che una delle finalità della norma è *«la rimozione dei principali ostacoli giuridici all'assolvimento, da parte delle istituzioni finanziarie, degli obblighi previsti dal FATCA (ad esempio, l'obbligo di chiusura dei conti dei clienti che non consentono la divulgazione delle informazioni che li riguardano – cosiddetti « recalcitrant » e la trasmissione diretta dei dati dei clienti all'Internal Revenue Service che avrebbe comportato la violazione della normativa europea sulla protezione dei dati personali)»*.
- Ai sensi del parere del WP, è decisamente troppo poco.

Questioni tuttora aperte

- Proporzionalità del trattamento
- Ruolo delle autorità fiscali interne e «secondary use» dei dati
- Informativa agli interessati
- Esercizio dei diritti di accesso e correzione
- Sicurezza e data breach
- Possibili dati sensibili
- Infine, ovviamente, trasferimento dei dati negli Stati Uniti: che tipi di garanzia esiste per il successivo trattamenti dei dati esportati (che non sono necessariamente solo di cittadini US)?

Dal FATCA al CRS

Nel maggio 2014, l'Organizzazione per la cooperazione e lo sviluppo economico («OCSE» in italiano o «OECD» in inglese) ha introdotto degli Common Reporting Standard (CSR) per lo scambio automatico di informazioni finanziarie (AEOI) attraverso il Global Forum on Transparency and Exchange of Information for Tax Purposes.

La dichiarata fonte di ispirazione è chiaramente il FATCA, tanto che il nuovo modello CRS è stato ironicamente ribattezzato "GATCA" (sta per Global FATCA).

Questioni privacy sulle OECD CRS

- Con parere del 18 settembre 2014, il WP ha affrontato anche le problematiche privacy delle CRS, assumendo una posizione critica: «the practical roll-out of CRS in Europe based on existing FATCA IT solutions currently lacks adequate data protection safeguards»
- “the mere act of adopting a national law and/or European law or international tax agreements providing for the possibility to use an automatic exchange of personal data under systems such as FATCA or CRS, would not alone be enough to ensure adequate data protection”.
- Peraltro, gli attuali modelli non sono conformi neppure alle Guidelines OECD on the Protection of Privacy and Transborder Flows of Personal Data, come riviste nel 2013

Tali rilievi sono stati confermati dal Segretario Generale dell’Autorità Garante dott. Brusia alla EBF – FBF Tax Conference del 22.9.14, a Parigi

Rilievi del WP sul modello CRS: questioni aperte

- Legal basis: It is essential that any law and agreement including the CRS contain substantive provisions that implement (and not just merely refer to) Directive 95/46/EC.
- Purpose limitation
- Necessity assessment under the proportionality principle
- Data retention
- Transparency and fair processing
- Data subjects' rights
- Controllershship
- Onward transfers
- Security measures
- Privacy Impact Assessment

Le nostre Sedi

In Italia...



Roma

Via delle Quattro
Fontane, 20
00184 Roma
Tel. +39 06 478751
Fax +39 06 4871101



Milano

Piazza Belgioioso, 2
20121 Milano
Tel. +39 02 763741
Fax +39 02 76009628



Bologna

Via Massimo
D'Azeglio, 25
40123 Bologna
Tel. +39 051 6443611
Fax +39 051 271669



Padova

Piazza Eremitani, 18
35121 Padova
Tel. +39 049 6994411
Fax +39 049 660341



Torino

C.so Vittorio
Emanuele II, 83
10128 Torino
Tel. +39 011 5660277
Fax +39 011 5185932

... e all'estero



Abu Dhabi

Penthouse 2102
CI Tower - 32nd St.
P.O. Box 42790
Abu Dhabi
Tel. +971 2 815 3333
Fax +971 2 679 6664



Brussels

184, Avenue Molière
B-1050 Brussels
Tel. +32 23401550
Fax +32 23401559



Hong Kong

Unit 208 - 2nd Floor
St. George's Building
2 Ice House Street
Central - Hong Kong
Tel. + 852 21563490
Fax + 852 21563499



London

6 - 8 Tokenhouse
Yard
London EC2R 7AS
Tel. +44 2073971700
Fax +44 2073971701



New York

1221 Avenue of the
Americas - 42nd Floor
New York, NY 10020
Tel. +1 212 957 9600
Fax +1 212 957 9608

Grazie per l'attenzione

Il presente documento è stato elaborato in modo indipendente da Gianni, Origoni, Grippo, Cappelli & Partners e consegnato a mero scopo informativo, pertanto, a causa dei continui cambiamenti di leggi, norme e regolamenti, potrebbe non essere aggiornato. Le informazioni qui contenute si basano su fonti ritenute attendibili e in buona fede. Tuttavia, non si rilascia nessuna dichiarazione o garanzia, espressa o implicita, né si garantisce l'imparzialità, l'accuratezza, la completezza o la correttezza delle informazioni contenute in questo documento. Questo documento, compresa ogni sua parte, non costituisce un riferimento per contratti o obblighi di alcun tipo, né può costituire in alcun modo una base affidabile per la conclusione di un accordo. Gianni, Origoni, Grippo, Cappelli & Partners non può essere ritenuto responsabile per eventuali danni, diretti o indiretti, derivanti dall'utilizzo del presente documento o del suo contenuto o comunque connessi al suo utilizzo. Il presente documento non può essere riprodotto, distribuito o pubblicato in tutto o in parte, per qualsiasi scopo, senza l'espressa autorizzazione da parte di Gianni, Origoni, Grippo, Cappelli & Partners. Per qualsiasi ulteriore chiarimento si prega di contattare Gianni, Origoni, Grippo, Cappelli & Partners.