ORDINE DEI GIORNALISTI DEL VENETO

Venezia, 11 aprile 2014

Libertà di espressione, sicurezza nazionale e diritti individuali

Prof. Maurizio Mensi

SSEF - Scuola Superiore dell'economia e delle finanze
Università LUISS "Guido Carli"
Roma

Sommario

- 1. Una “dirompente innovazione”. Equilibrio tra sicurezza e *privacy* nell'era digitale
- 2. Le sfide della sorveglianza delle comunicazioni. La *privacy* come un diritto qualificato. Sfera privata e interesse pubblico
- 3. Standard normativi internazionali
- 4. La fiducia pubblica nell’economia digitale e la protezione dei dati
- 5. L’Unione europea e il Consiglio d'Europa
- 6. Il regime giuridico italiano: *privacy*, sicurezza, controllo
- 7. La sicurezza nazionale
- 8. Nuove sfide: *targeting* comportamentale, *cloud computing*, violazione dati
- 9. La protezione dati in Regno Unito, Francia e Germania
- 10. USA e UE: un approccio diverso
- 11. La riforma EU e la revisione della Convenzione n.108 del Consiglio d'Europa

1- Un'innovazione dirompente

- *"A disruptive innovation"* (C.Christensen, 1995)
- Le innovazioni tecnologiche hanno aumentato le possibilità di comunicazione e di protezione della libertà d'espressione e di opinione, consentendo di agire nell'anonimato, attraverso un rapido scambio di informazioni che favorisce il dialogo interculturale. Ma **i cambiamenti tecnologici facilitano contemporaneamente il controllo dello Stato sulle comunicazioni private tra individui.**
- Attraverso la comunicazione, le informazioni più personali e intime, siano esse attinenti ad un singolo o ad un gruppo, possono essere rivelate.

2- L’avvento di Internet

- Il passaggio dai sistemi di telefonia fissa di telecomunicazione mobile all’era di Internet e i costi in declino dei servizi di comunicazione hanno provocato una crescita esponenziale dell’uso del telefono cellulare. **L'avvento di Internet** ha visto la nascita di una serie di nuovi strumenti e applicazioni per comunicare a costo zero oppure a prezzi molto convenienti.
- Gli Stati hanno dunque ricalibrato le proprie infrastrutture tecnologiche al fine di includere funzionalità di i**ntercettazione** (“*backdoors*”) per consentire una maggiore sorveglianza, rendendo le reti telefoniche moderne accessibili in remoto e controllabili.

3- L'uso dei dati da parte delle autorità statali è in gran parte non regolamentato

- La natura dinamica della tecnologia non solo ha cambiato il modo in cui la sorveglianza può essere effettuata, ma anche "**cosa**" **può essere monitorato**. Consentendo la creazione di varie modalità di comunicazione e condivisione di informazioni, Internet ha anche facilitato lo sviluppo di grandi quantità di dati scambiati a livello transnazionale da parte dei singoli.
- Rif. "Apocalisse informativa". Il consumismo informativo come minaccia per la democrazia. E.Morozov, Il mercato dei dati, in Internazionale, settembre 2013

4- L'uso dei dati da parte delle autorità statali è in gran parte non regolamentato (2)

- Queste informazioni, cd. **comunicazioni di dati o *metadati*** (i dati estrinseci relativi alle telefonate effettuate e/o ricevute, esclusi i contenuti), contengono informazioni personali sugli individui, la loro posizione e attività *on-line*, e informazioni relative alle *e-mail* e messaggi che inviano o ricevono. Le comunicazioni di dati sono memorizzabili, accessibili e consultabili, e il loro l'utilizzo da parte delle autorità statali è **in gran parte non regolamentato**. L'analisi di questi dati può essere altamente invasiva, in particolare quando i dati vengono combinati e aggregati

5- Le sfide per la sicurezza nazionale

- I timori per la sicurezza nazionale e le attività criminali possono giustificare l'utilizzo eccezionale di tecnologie di sorveglianza delle comunicazioni. Tuttavia, le norme che dovrebbero regolare un intervento statale che **sia necessario, legittimo e proporzionato** nella sorveglianza delle comunicazioni sono spesso inadeguate o inesistenti. L'inadeguatezza del regime giuridico domestico crea un terreno fertile per le violazioni arbitrarie e illegali del diritto alla *privacy* nelle comunicazioni e, di conseguenza, costituisce una minaccia per la tutela del diritto alla libertà di opinione e di espressione.

6- Un equilibrio tra sicurezza nazionale e privacy?

- E 'possibile trovare un equilibrio tra la tutela della sicurezza nazionale e il rispetto della privacy?
- Le innovazioni tecnologiche si sono sviluppate parallelamente ad un mutamento negli atteggiamenti verso la sorveglianza delle comunicazioni. Quando la pratica delle intercettazioni ebbe inizio negli **Stati Uniti d'America**, era condotta in base a criteri molto rigidi.
- Nella prima convalida giudiziaria delle intercettazioni, il giudice Brandeis della **Corte Suprema degli Stati Uniti** espresse un netto dissenso rilevando che le intercettazioni costituivano un "mezzo di vasta portata suscettibile di violare la *privacy*" e dunque difficilmente giustificabile ai sensi della Costituzione (1928) .
- Le intercettazioni erano percepite come un mezzo estremamente rischioso per la *privacy*, il cui uso doveva essere limitato a individuare e perseguire i reati più gravi .

7- Le ragioni della sorveglianza nell'era digitale

- Nel corso del tempo, tuttavia, gli Stati hanno ampliato i loro poteri di sorveglianza, abbassando la soglia di tutela della privacy e **aumentando le cause giustificatrici dell'esercizio di tali poteri di monitoraggio.**
- In molti paesi, la legislazione e le prassi esistenti non sono state riviste e aggiornate per affrontare le minacce e le **sfide poste dalla sorveglianza delle comunicazioni nell'era digitale**.

8- L'autorizzazione giudiziaria e la vigilanza indipendente

- L'assenza di leggi che regolamentino gli accordi internazionali di sorveglianza e di condivisione delle comunicazioni ha generato **pratiche *ad hoc* che sfuggono al controllo di un'autorità indipendente.**
- Oggi in molti Stati membri l'accesso ai dati di comunicazione può essere condotto da una vasta gamma di **enti pubblici** per una moltitudine di scopi, spesso senza l'autorizzazione giudiziaria o una supervisione indipendente.
- Inoltre gli Stati hanno cercato di adottare meccanismi di sorveglianza che tendono ad avere effetto extraterritoriale.

9- Privacy

- A livello internazionale **la *privacy* è** riconosciuta come un diritto umano fondamentale.
- Il diritto alla *privacy* è sancito dalla **Dichiarazione universale dei diritti dell'uomo** - 1948 (art. 12), dal **Patto internazionale sui diritti civili e politici** - 1966 (ICCPR, Art. 17 .), dalla **Convenzione sui diritti del fanciullo** - 1989 (art. 16), e dalla **Convenzione internazionale sulla protezione di tutti i lavoratori migranti e dei membri delle loro famiglie** - 1990 (art. 14) .
- Il diritto alla *privacy* è protetto altresì dalla **Convenzione europea dei diritti dell'uomo** - 1950 (art. 8) e dalla **Convenzione americana sui diritti umani** - 1969 (art. 11).

10- I diritti fondamentali

- In **Europa** il diritto alla *privacy* e il diritto alla protezione dei dati costituiscono diritti fondamentali. La **Convenzione europea dei diritti dell'uomo** (1953) tutela il diritto alla vita privata, mentre il diritto alla protezione dei dati è sancito dalla **Carta dei diritti fondamentali dell'Unione europea** (2009) .
- La **Carta dei diritti fondamentali dell'Unione europea** protegge i dati personali sancendo che "*Ogni individuo ha diritto alla protezione dei dati personali che lo riguardano*" (art. 8.1)

11- I diritti fondamentali (2)

- La **direttiva sulla protezione dei dati del 1995 (95/46)** impone agli Stati membri dell'Unione europea di dare attuazione alle norme specifiche sulla protezione dei dati. Le persone i cui dati sono in corso di elaborazione godono di più diritti, mentre i soggetti che trattano i dati personali hanno una serie di obblighi. Le **Autorità indipendenti di protezione dei dati** debbono invece vigilare sul rispetto delle regole.
- Le norme europee sulla protezione dei dati si applicano allorquando una società si trova ad elaborare dei dati cd. “personali”.

12- La sfera privata e l'interesse pubblico

- Poiché il diritto alla *privacy* è un diritto qualificato, la sua interpretazione pone delle sfide rispetto alle nozioni di "**sfera privata**" e "**interesse pubblico**".
- La *privacy* può essere definita come la garanzia che gli individui abbiano una **sfera di sviluppo autonomo, interazione e libertà**, immune dall'intervento dello Stato e di altri soggetti terzi.
- Il diritto alla *privacy* è anche la capacità degli individui di determinare chi detiene le informazioni su di loro e come tali informazioni vengono utilizzate.

13- La diminuzione dei costi della sorveglianza

- **I costi e gli ostacoli logistici della sorveglianza su ampia scala continuano a diminuire rapidamente**, favorendo la proliferazione delle tecnologie di intercettazione, monitoraggio e analisi delle comunicazioni. Oggi, alcuni Stati membri hanno la capacità di **monitorare e registrare le comunicazioni telefoniche e *on-line* su scala nazionale**, mettendo dei **filtri sui cavi in fibra ottica** attraverso cui la maggior parte delle informazioni digitali circolano, e applicando meccanismi di riconoscimento vocale o di parole.
- Tali meccanismi sarebbero stati adottati, ad esempio, dal **governo egiziano** e da quello **libico** nel periodo che ha preceduto la primavera araba.
- In molti Stati la conservazione obbligatoria dei dati sta facilitando la raccolta massiccia di dati di comunicazione che possono essere successivamente filtrati e analizzati a vari fini.

14- L'esame approfondito dei pacchetti

- "**Scatole nere**" possono essere progettate per controllare il flusso di dati attraverso Internet, al fine di filtrare e ricostruire tutte le informazioni sulle attività *on-line*. Questo metodo, chiamato "***deep-packet inspection***", consente allo Stato di conoscere non solo quali siti vengano visitati dagli utenti, ma il contenuto dei siti stessi. Tale tecnologia è stata largamente usata dagli stati interessati dalle recenti rivolte popolari nella regione del **Medio Oriente** e del **Nord Africa.**
- Un altro strumento utilizzato regolarmente dagli Stati oggi è il **monitoraggio dei *social media***.
- Gli Stati hanno inoltre acquisito i mezzi tecnici per ottenere *username* e *password* da siti di *social networking*.

15- Gli standard normativi

- Nella maggior parte degli Stati, **le norme giuridiche in materia di sorveglianza delle comunicazioni sono inadeguate o addirittura inesistenti.**
- Gli Stati cercano dunque di trovare un ancoraggio normativo che legittimi le loro azioni di monitoraggio sulle informazioni all'interno degli **istituti giuridici tradizionali**, senza riconoscere che la tecnologia utilizzata spesso esula dall'ambito di applicazione di tali norme. Progressivamente, la sorveglianza delle comunicazioni viene sempre più **autorizzata su base più ampia e indiscriminata**, senza la necessità per le autorità incaricate dell'applicazione della legge di individuare la base fattuale che giustifichi tale potere di sorveglianza caso per caso.
- Molti Stati permettono alle **forze dell'ordine** di non dover sottostare alla permanente supervisione dell'autorità giudiziaria dopo aver ottenuto l'emissione di un ordine di intercettazione. Alcuni Stati impongono **limiti temporali all'esecuzione degli ordini di intercettazione,** ma consentono alle autorità incaricate dell'applicazione della legge di rinnovare tali ordini ripetutamente e indefinitamente.

16- Il Regno Unito

- In alcuni paesi, l'intercettazione delle comunicazioni può essere autorizzata da un ministro del governo, un suo delegato, o da una commissione. Nel **Regno Unito** l'intercettazione delle comunicazioni è autorizzata dal Segretario di Stato (sezione 5 *Regulation of Investigatory Powers Act*, 2000)
- Oltre 200 agenzie, le forze di polizia e le autorità carcerarie sono autorizzate ad acquisire i dati delle comunicazioni ai sensi del *Regulation of Investigatory Powers Act* del 2000. Di conseguenza, è difficile per i singoli prevedere quando e da parte di quale agenzia dello Stato potrebbero essere sottoposti a sorveglianza.

17- Colombia

- In molti Stati, i fornitori di servizi di comunicazione sono stati costretti a modificare le proprie infrastrutture per consentire la sorveglianza diretta, eliminando la possibilità di supervisione giudiziaria. Ad esempio, nel **2012** i **Ministeri della Giustizia e quello delle Tecnologie dell'Informazione e della Comunicazione della Colombia** hanno adottato un decreto che ha imposto ai fornitori di servizi di telecomunicazioni di sviluppare delle infrastrutture che consentano l'accesso diretto alle comunicazioni da parte della polizia giudiziaria, senza bisogno di un intervento del Procuratore Generale.

18- India

- Il **governo indiano** sta proponendo di installare un sistema di monitoraggio centralizzato che indirizzerà tutte le comunicazioni al governo centrale, permettendo alle **agenzie di sicurezza** di bypassare l'interazione con il fornitore di servizi.
- Tali accordi mantengono la sorveglianza delle comunicazioni al di fuori dell'ambito di autorizzazione giudiziaria e permettono una sorveglianza non regolamentata, occulta, eliminando qualsiasi garanzia di trasparenza e assunzione di responsabilità da parte dello Stato.

19- Il caso *Datagate*

- Intercettazioni di massa disposte con il programma *"**Prism**"* dall'Agenzia per la sicurezza nazionale (NSA), emerse in seguito alle rivelazioni dell'analista **Edward Snowden**.
- ***Foreign Intelligence Surveillance Court***.
- La Sezione 215 del ***Patriot Act*** (2001), per esempio, ha modificato alcune disposizioni del ***Foreign Intelligence Surveillance Act*** (1978), consentendo l'accesso alle registrazioni di informazioni detenute dagli ***Internet Service Provider*** (ISP), una volta ottenuta l'approvazione giudiziaria .
- Il problema del rispetto del **Primo Emendamento del *Bill of Rights* della Costituzione degli Stati Uniti**, che protegge la libertà di parola e la libertà di associazione, e il **Quarto Emendamento** tutela la *privacy*.
- **Il caso Echelon e il caso USA del 2005**

20- Il caso *Datagate*- Il seguito (1)

- Il **27 agosto 2013** il Presidente Obama ha annunciato l'istituzione di un Gruppo di lavoro, con il compito di esaminare il sistema di "*Intelligence*" e proporre i necessari interventi di revisione.
- Il Gruppo ha presentato, il **12 dicembre 2013**, il rapporto "***Libertà e sicurezza in un mondo che cambia***", contenente **46 raccomandazioni**: occorre precisare, e in alcuni casi stabilire *ex novo,* condizioni, parametri giuridici e modalità per il legittimo svolgimento degli interventi di sorveglianza e raccolta delle informazioni e operare alcuni puntuali interventi di riforma.
- Il **17 gennaio 2014** il Presidente Obama ha recepito gran parte dei suggerimenti, con la direttiva "***Signal Intelligence Activities***".

21- Il caso *Datagate*- Il seguito (2)

- Le **agenzie di sicurezza americane**, ***in primis*** **la NSA,** non potranno più accedere direttamente ai tabulati telefonici dei cittadini americani, e sono previsti precisi limiti giuridici alla capacità del governo di accedere a tali informazioni.
- Per ogni richiesta da parte del governo di acquisire un meta-dato (i dati estrinseci relativi alle telefonate effettuate e/o ricevute, esclusi i contenuti) sarà necessario **un ordine del giudice.**
- Si prevede l'istituzione di un nuovo soggetto (che potrà essere pubblico o privato), esterno al governo, sottoposto a disciplina e controlli rigorosi, a cui sarà affidata la conservazione di tutti i dati raccolti (Sez. 2)

22- Il caso *Datagate* – Il seguito (3)

- Sono introdotte restrizioni alla possibilità di controllare **Paesi alleati, e i Capi di Stato** sono esclusi da qualsiasi forma di sorveglianza elettronica. Si stabiliscono condizioni rigide affinché alle informazioni più delicate accedano soltanto i funzionari a ciò autorizzati. Tutti i dati raccolti sono sottoposti a più puntuali condizioni di sicurezza (Sez. 4, lett. s) ii).
- L'effettiva sussistenza delle "***legittime esigenze di sicurezza nazionale***" appare uno degli elementi centrali della riforma, in quanto condizione e presupposto per la raccolta di informazioni, anche commerciali, riservate (Sez. 1, lett. c).

23- La protezione dei dati personali e la sicurezza

- Le **direttive europee** del 2002, in materia di comunicazioni elettroniche: un elevato livello di protezione della vita privata e dell'integrità delle reti di telecomunicazione.
- La **Convenzione dei Diritti dell'Uomo** (1950) consente di limitare la libertà per motivi di sicurezza.
- **Comitato dei Ministri**: Raccomandazione e Dichiarazione (2005) sulle tecniche d'indagine e la lotta contro il terrorismo.

24- Italia

- Il **Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 2003)**
- I dati raccolti dagli operatori telefonici devono essere conservati per **due anni,** altre tipologie di dati (ad esempio i messaggi *e-mail* o *sms*) per 1 anno. **Vedasi sent. CGUE 8 aprile 2014. C 293/12 e C594/12.**
- **L'intercettazione del contenuto radiotelefonico è ammessa solo in caso di autorizzazione giudiziaria.**
- Non sono ammesse le cd. "*fishing expedition*", salvo vi siano esigenze di prevenzione del terrorismo e tutela della sicurezza dello Stato. Il **Presidente del Consiglio dei Ministri** può delegare i Capi dei Dipartimenti di sicurezza, previa autorizzazione del Procuratore della Repubblica presso la Corte di Appello di Roma, a operare intercettazioni delle comunicazioni su larga scala (**Legge n. 155 del 2005**).

25- Le eccezioni di sicurezza nazionale

- Il concetto vago e non determinato di **"sicurezza nazionale"** costituisce una causa di giustificazione accettabile per l'intercettazione e l'accesso alle comunicazioni in molti paesi.
- In **India**, per esempio, l'*Information Technology Act* del 2008 consente l'intercettazione delle comunicazioni nell'interesse, *inter alia*, "*della sovranità, integrità o difesa dell'India, delle sue relazioni amichevoli con gli Stati esteri, dell'ordine pubblico e delle esigenze di investigazione di qualsiasi reato*"(sezione 69).

26- USA, Germania e Svezia

- Negli **Stati Uniti**, il ***Foreign Intelligence Surveillance Act*** autorizza la **NSA, *National Security Agency*** a intercettare senza autorizzazione giudiziaria le comunicazioni in cui una parte si trovi al di fuori degli Stati Uniti, ed uno dei partecipanti sia ragionevolmente sospettato di appartenere ad un'organizzazione designata come "terroristica".
- In **Germania** la legge consente l'intercettazione senza mandato di comunicazioni nazionali ed internazionali da parte dei servizi di *intelligence* statali per fini di tutela dell'ordine democratico libero, dell'esistenza e della sicurezza dello Stato.
- In **Svezia**, la legge sulla *Signals Intelligence in Defense Operations* autorizza l'agenzia di *intelligence* ad intercettare, senza alcun mandato o ordine del tribunale, tutto il traffico telefonico e Internet che si svolga all'interno dei confini del paese.

27- L'applicazione extraterritoriale delle leggi di sorveglianza

- In risposta ai crescenti flussi transnazionali di dati, un certo numero di Stati ha iniziato ad adottare leggi che permettono loro di porre in essere una sorta di **sorveglianza extra-territoriale o intercettare le comunicazioni in giurisdizioni estere.**
- In **Sud Africa**, il *General Intelligence Laws Amendment Bill* autorizza la sorveglianza delle comunicazioni estere al di fuori del Sud Africa o dei flussi di informazioni che attraversano il paese.
- Nel mese di **ottobre 2012**, il **ministero olandese di Giustizia e Sicurezza** ha proposto alcune modifiche legislative al Parlamento nazionale che permetterebbero alla polizia di investigare il contenuto di computer e telefoni cellulari, sia all'interno dei Paesi Bassi sia all'estero, al fine di installare *spyware*, identificare e distruggere i dati.

28- Pakistan e Stati Uniti d'America

- Nel **dicembre 2012,** l'Assemblea nazionale del **Pakistan** ha approvato il ***Fair Trial Act***, che prevede, al paragrafo 31, l'esecuzione dei mandati di sorveglianza in giurisdizioni estere.
- Nello stesso mese, gli **Stati Uniti** hanno rinnovato il ***Foreign Intelligence Surveillance Amendment Act*** **del 2008**, che proroga il potere del governo di sorvegliare i soggetti non americani localizzati fuori degli Stati Uniti (§1881a), ivi incluso qualsiasi individuo straniero le cui comunicazioni siano ospitate da servizi di ***cloud computing*** che si trovino negli Stati Uniti (come *Google* e altre grandi aziende).

29- Lo European Telecommunications Standards Institute (ETSI)

- Nel 2012, l'***European Telecommunications Standards Institute*** (ETSI) ha elaborato degli standard per l'intercettazione dei servizi stranieri di ***cloud computing*** da parte dei governi europei.
- Questi sviluppi suggeriscono una tendenza verso l'estensione dei poteri di sorveglianza oltre i confini territoriali nazionali, aumentando il rischio di accordi di cooperazione tra le agenzie di sicurezza dei vari Stati che permettano di eludere le garanzia normative previste dalle norme nazionali.

30- I regimi normativi delle misure di sorveglianza

- I regimi normativi in materia debbono **garantire che le misure di sorveglianza delle comunicazioni**:
- a) siano stabilite dalla legge, avente un livello di **chiarezza e di precisione** tale da assicurare che gli individui ne abbiano contezza e possano prevederne applicazione;
- b) siano strettamente e manifestamente **necessarie per raggiungere uno scopo legittimo**; e
- c) rispettino il **principio di proporzionalità**, e non vengano impiegati quando vi siano misure meno invasive disponibili e non siano ancora state utilizzate.

31- I regimi normativi delle misure di sorveglianza (2)

- Gli Stati dovrebbero **criminalizzare la sorveglianza non autorizzata posta in essere da soggetti pubblici o privati**. Tali norme non devono essere utilizzate per colpire i cd. *whistleblowers* o altri soggetti che cercano di denunciare violazioni di diritti umani, né devono ostacolare la legittima sorveglianza sull'azione di governo da parte dei cittadini.
- Il conferimento dei dati di comunicazione allo Stato deve essere monitorato da un'**autorità indipendente**.
- A livello internazionale, gli Stati dovrebbero adottare meccanismi di Mutua Assistenza Legale per regolare l'accesso ai dati sulle comunicazioni detenuti da soggetti societari esteri.

32 - La Dichiarazione del Comitato dei Ministri sui rischi per i diritti fondamentali

- **Dichiarazione del Comitato dei Ministri sui rischi per i diritti fondamentali derivanti dal monitoraggio digitale e altre tecnologie di sorveglianza** (11 giugno 2013) .
- Questi strumenti e pratiche possono avere un effetto deterrente sulla partecipazione dei cittadini alla vita sociale, culturale e politica e, nel lungo periodo, potrebbero avere effetti dannosi sulla democrazia. Essi possono anche pregiudicare i diritti di riservatezza connessi ad alcune professioni, come la protezione delle fonti dei giornalisti, e persino minacciare la sicurezza dei soggetti interessati.
- **Strumenti di *tracking* e tecnologie di sorveglianza** possono essere utilizzati nel perseguimento di interessi legittimi, ad esempio per sviluppare nuovi servizi, migliorare l'esperienza *on-line* dell'utente o facilitare la gestione della rete, e l'applicazione della legge stessa. D'altra parte, possono essere utilizzati anche per fini illeciti favorendo un accesso non autorizzato ai dati, intercettazioni e interferenze, meccanismi di sorveglianza del sistema informatico, o altre forme di abuso.

33- La Direttiva UE relativa agli attacchi contro i sistemi di informazione

- La **direttiva 2013/40 del 12 agosto 2013** relativa agli attacchi contro i sistemi di informazione.
- **Obiettivi**: armonizzazione del diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione attraverso la definizione di standard minimi circa la definizione dei reati e delle relative sanzioni e miglioramento della cooperazione tra le autorità competenti, comprese le forze di polizia e gli altri servizi incaricati dell'applicazione della legge, nonché le competenti agenzie dell'Unione e gli organismi specializzati, come *Eurojust*, *Europol* e l'*European Network and Information Security Agency* (ENISA).

34- L'importanza dei sistemi di informazione

- **I sistemi di informazione sono un elemento chiave di interazione politica, sociale ed economica nell'UE**. La società è altamente e sempre più dipendente da tali sistemi. Il loro buon funzionamento e loro sicurezza sono di vitale importanza per lo sviluppo del mercato interno europeo e di un'economia competitiva e innovativa.
- Vi è la necessità di **sviluppare un approccio comune agli elementi costitutivi dei reati** con l'introduzione di reati comuni di accesso illecito ad un sistema di informazione, interferenza illecita nei sistemi di comunicazione elettronica, interferenza illecita di dati e intercettazione illecita.
- **Gli attacchi informatici su larga scala** possono causare un danno economico rilevante sia attraverso l'interruzione dei sistemi informativi e di comunicazione sia attraverso la perdita o l'alterazione di informazioni commercialmente rilevanti o confidenziali.

35- Il potenziamento della sicurezza dei sistemi informativi

- L'identificazione e la segnalazione delle minacce e dei rischi derivanti da attacchi informatici e dalla vulnerabilità dei sistemi di informazione sono elementi efficaci di prevenzione, e costituiscono la risposta agli **attacchi informatici** e all'esigenza di miglioramento della sicurezza dei sistemi informativi. Occorre dunque prevedere incentivi per la segnalazione delle eventuali lacune nella sicurezza dei sistemi di comunicazione elettroniche.

36- Italia. Recenti sviluppi. La protezione cibernetica

- dPCM 24 gennaio 2013. **Direttiva sugli indirizzi per la protezione cibernetica e la sicurezza informatica nazionale**
- 20 febbraio 2014, pubblicazione del:

- **Piano nazionale per la protezione cibernetica e la sicurezza informatica, promosso dalla presidenza del Consiglio dei ministri**;

- **Quadro strategico nazionale per la sicurezza dello spazio cibernetico**.

Approvati dal Comitato interministeriale per la sicurezza della Repubblica (CISR) e adottati dal Presidente del Consiglio dei ministri.

L'Italia si dota così di una strategia organica per "*prevenire le future minacce atte a minare lo sviluppo economico, sociale, scientifico e industriale, nonché la stabilità politico-militare*".

37- La protezione cibernetica in Italia (2)

- **Obiettivi**: potenziare le capacità di difesa delle infrastrutture critiche nazionali, incentivare la cooperazione tra istituzioni ed imprese nazionali, promuovere la cultura della sicurezza cibernetica, rafforzare la cooperazione internazionale
- Il **crimine informatico** *"è una piaga che può decretare il fallimento delle aziende, la sottrazione del loro patrimonio tecnologico e che depaupera la ricchezza delle nazioni. Con sempre maggiore preoccupazione assistiamo inoltre al crescere di una minaccia ancora più insidiosa, che sfrutta la* ***vulnerabilità dei sistemi informatici*** *per sottrarre il frutto del nostro lavoro di ricerca e sviluppo nel campo delle nuove tecnologie e dei prodotti. Per un Paese come l'Italia, che fa dell'innovazione la pietra angolare della sua crescita e della sua competitività, il danno potenziale è incalcolabile*".

38- La protezione cibernetica in Italia (3)

- **Nuova struttura** per fronteggiare la cyber-minaccia:

- Presidente del Consiglio, adotta il Piano ed il Quadro Strategico, supportato dal Comitato interministeriale per la sicurezza della Repubblica (Cisr).
- La prevenzione di crisi e l'attivazione delle procedure di allertamento, risposta e ripristino spetta al **Nucleo per la sicurezza cibernetica (Ncs)** istituito nell'ambito dell'Ufficio del Consigliere militare del presidente del Consiglio.
- Se l'evento è di dimensioni tali da incidere sulla sicurezza nazionale o non può essere fronteggiato dalle amministrazioni competenti, il Nucleo dichiara la situazione di crisi cibernetica ed attiva il **Nucleo interministeriale situazione e pianificazione (Nisp).**

39- Il *targeting* comportamentale

- Il cd. ***on-line profiling*** è un argomento dibattuto.
- Gran parte della raccolta di dati personali su Internet è legata al *targeting* comportamentale, nonostante studi indicano che la maggior parte della popolazione non vuole ricevere pubblicità comportamentale mirata. Il ***World Wide Web Consortium*** sta discutendo una norma "***Do Not Track***", e le autorità di regolamentazione di tutto il mondo stanno sforzandosi per trovare risposte in tal senso.

40- Il *targeting* comportamentale (2)

- Il *targeting* comportamentale consiste nel monitoraggio del comportamento *on-line* degli utenti al fine di utilizzare le informazioni raccolte per indirizzare gli individui tramite pubblicità che siano corrispondenti ai loro interessi precedentemente individuati.
- Diverse tecnologie possono essere utilizzate per il *targeting* comportamentale , ad esempio i ***cookie***, i "***super cookies***", **dispositivi di "*fingerprinting*"** e l'**esame approfondito dei pacchetti** (*Deep packet inspection* - DPI). Peraltro l'eliminazione dei *cookie* non è sempre sufficiente ad evitare la tracciabilità.

41- *Targeting* comportamentale e diritto europeo

- Le norme sulla protezione dei dati europei, o quelle sulla privacy, trovano applicazione nei confronti del *targeting* comportamentale nella maggior parte dei casi.
- La Direttiva sulla protezione dei dati definisce i "**dati personali**" come "qualsiasi informazione concernente una persona fisica identificata o identificabile" (cd. "*data subject*"). Una persona è identificabile quando può essere direttamente o indirettamente identificata.
- Il preambolo della direttiva sancisce che per determinare se una persona è identificabile, è opportuno tener conto di tutti i mezzi che possono essere ragionevolmente utilizzati sia dalla [società] o da qualsiasi altra persona per identificare detta persona" (Art. 2(a) e considerando 26). Quindi, non è determinante che si tratti di una società in possesso di dati o d'un'altra parte in grado di identificare una persona.

42- La Corte di giustizia e le autorità di protezione dei dati dell'UE

- La **Corte di giustizia dell'Unione europea** non si è ancora pronunciata sul *targeting* comportamentale.
- La discussione sul *targeting* comportamentale è simile al dibattito sugli indirizzi IP. In una decisione del 2011 concernente gli indirizzi IP nelle mani di un fornitore di accesso a Internet, la Corte ha affermato che tali **indirizzi IP costituiscono dati personali**. La Corte ha così confermato che anche le informazioni senza nome possono essere considerate "dati personali".
- Le autorità europee di protezione dei dati nazionali ritengono che i **dati che consentono di distinguere una persona all'interno di un gruppo** costituiscono "dati personali".

43- La Corte di giustizia e le autorità di protezione dei dati dell'UE (2)

- Anche i ***cookies*** utilizzati per il *targeting* comportamentale sono dati personali perché consentono alle persone interessate di essere individuate, anche se i loro veri nomi non sono noti.
- Le norme sulla protezione dei dati si applicano al *targeting* comportamentale nella maggior parte dei casi.
- Nel **gennaio 2012,** la Commissione europea ha presentato una **proposta di regolamento sulla protezione dei dati** che dovrebbe sostituire la **direttiva del 1995.** La definizione di dati personali proposta include gli "identificatori *on-line*" nella lista di esempi che possono essere utilizzati per identificare una persona.

44- Il *Cloud Computing*

- Il *cloud computing* è un concetto molto ampio.
- I **servizi di *cloud computing*** offerti e i modelli di *cloud computing* (pubblico e privato) sono di vario genere.
- Di conseguenza, i problemi e le preoccupazioni variano a seconda dei servizi e modelli coinvolti. **Non è sempre evidente ove i dati si trovano e sono memorizzati** (per esempio in diversi *server*, anche virtuali), **chi ha accesso ai dati, da chi i dati vengono gestiti, chi è responsabile per l'elaborazione degli stessi e che tipo di processi di *back-up* e di ripristino sono stati messi in atto.** Tuttavia, risposte chiare a queste domande sono necessarie per garantire la sicurezza e la riservatezza del trattamento dei dati.
- In base al parere del **Garante europeo della protezione dei dati** sulla "***Protezione dei dati e il cloud computing ai sensi del diritto comunitario*" del 13 aprile 2010** gli obblighi di riservatezza e di sicurezza sono vincolanti per tutti coloro che trattano dati personali.

45- Trasferimenti internazionali di dati

- Un fornitore di servizi di ***cloud*** stabilito nell'UE, o in qualità di responsabile dei dati per un *controller* stabilito nella UE, in linea di principio, ricade nell'ambito di applicazione del **diritto dell'Unione**.
- Anche un fornitore di ***cloud*** che utilizza apparecchiature (come i *server*) in uno Stato membro dell'UE, o agisce in qualità di responsabile dei dati per un *controller* con tali apparecchiature, è tenuto al rispetto del diritto dell'Unione. Diversamente, un fornitore di servizi di *cloud*, pur nel caso in cui si rivolga principalmente ai cittadini europei, non sarebbe interessato dal diritto comunitario.
- Un importante problema riguarda i **trasferimenti internazionali di dati**. L'articolo 25 della direttiva sulla protezione dei dati vieta i trasferimenti di dati personali verso paesi che non garantiscono un livello adeguato di protezione.
- Tuttavia, la **circolazione dei dati personali all'interno o all'esterno della *cloud*** può verificarsi in **paesi non-EU/EEA**, la maggior parte dei quali non forniscono un adeguato livello di protezione.

46- La disciplina normativa sulla protezione dei dati in EU e USA

- **La disciplina normativa sulla protezione dei dati varia tra l'Unione europea e gli Stati Uniti. In generale, la legislazione dell'UE risulta essere più rigorosa** .
- Per soddisfare il livello di protezione richiesto dalla direttiva dell'UE, il *Department of Commerce* (DOC) statunitense ha redatto i "***Safe Harbor*" *Privacy Principles*.**
- Questo strumento è particolarmente rilevante in quanto i principali fornitori di servizi di ***cloud computing*** sono basati negli Stati Uniti.
- Nel 2000, la CE ha recepito tali principi. Tuttavia, i principi "*Safe Harbor*" sono stati bersaglio di molte critiche per quanto riguarda la loro applicazione e rispetto..

47- EU e USA

- La UE riconosce anche **Svizzera, Canada, Argentina, Jersey, Guernsey e l'Isola di Man**, come paesi aventi un livello adeguato di protezione dei dati.
- Ai sensi del ***Patriot Act* statunitense**, ai fini delle indagini anti-terrorismo, i funzionari americani possono accedere alle informazioni concernenti cittadini di altri paesi se tali informazioni sono fisicamente negli Stati Uniti o sono accessibili per via telematica.
- Inoltre, pare che in generale alcuni "**interessi economici strategici degli Stati Uniti**" acquisiscano priorità rispetto ai principi "*Safe Harbor*".
- Questo approccio è stato confermato quando, nel giugno 2011, il capo di ***Microsoft* UK** ha ammesso per la prima volta di non poter garantire che i dati EU, memorizzati e conservati nei *data center* in territorio europeo, non lascino l'UE a fronte di una richiesta presentata ai sensi del *Patriot Act*.

48- Le violazioni dei dati

- **Regolamento della Commissione n ° 611/2013 del 24 giugno 2013** sulle misure applicabili alla notifica delle violazioni dei dati personali (“***Data breach notification”)*** ai sensi della Direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche.
- I fornitori di servizi di comunicazione elettronica accessibili al pubblico sono tenuti a notificare alle autorità nazionali competenti, e in alcuni casi anche agli abbonati e agli individui interessati, le **violazioni dei dati personali**.

49- Le violazioni dei dati (2)

- Le violazioni dei dati includono: le violazioni della sicurezza che portano alla distruzione accidentale o illecita, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione elettronica accessibile al pubblico.
- I requisiti nazionali diversi possono favorire l'incertezza giuridica, procedure più complesse e onerose e significativi costi amministrativi per i fornitori che operano a livello transfrontaliero.
- I fornitori dovrebbero notificare all'autorità nazionale competente tutte le violazioni di dati personali. Pertanto, nessun margine di discrezionalità deve essere lasciato al fornitore circa l'obbligo di notifica della violazione all'autorità nazionale competente.

50- Il meccanismo di notifica delle violazioni dei dati personali

- Un sistema di notifica delle violazioni dei dati personali all'autorità nazionale competente è costituito da varie fasi, ciascuna soggetta a determinati limiti di temporali.
- Questo sistema garantisce che **l'autorità nazionale competente venga informata quanto prima e nel modo più accurato possibile**, senza però ostacolare indebitamente il fornitore nei suoi sforzi di indagare la violazione e di adottare le misure necessarie per circoscriverla e porvi rimedio.
- Ai fini della sussistenza di una violazione dei dati personali non è sufficiente un semplice sospetto né una semplice rilevazione di un incidente non supportata da informazione adeguate.
- Le autorità nazionali competenti interessate dovrebbero collaborare in caso di violazioni di dati personali aventi una dimensione transfrontaliera.

51- L'esecuzione delle norme circa la protezione dei dati nel Regno Unito, Francia e Germania

- Il ***Data Protection Act* francese** (legge 78-17 del 6 gennaio 1978, come modificata), prevede un Comitato e un presidente aventi una vasta gamma di poteri esecutivi.
- Nel caso in cui le società non riescano ad adempiere i loro obblighi ai sensi della legge, il Comitato può emettere un "avviso" al titolare, che è considerato alla stregua di una sanzione.
- In alternativa, il presidente può anche emanare un'intimazione a conformarsi alle norme. Nel caso in cui le società non diano seguito a tale intimazione, il comitato può, previa audizione delle parti, imporre un'ingiunzione alle imprese di cessare il trattamento o revocare l'autorizzazione al trattamento dei dati, ove concessa, o imporre una multa.
- Il *Data Protection Act* francese pone limiti alle sanzioni pecuniarie che possono essere applicate alle società inadempienti.

52- Germania

- Per quanto riguarda le norme sulla protezione dei dati applicabile alle società private, la **legge sulla protezione dei dati tedesca** è la stessa in tutti i 16 Stati federali del paese.
- La legislazione sulla protezione dei dati tedesca prevede che le Autorità dello Stato abbiano una serie di poteri in termini di esecuzione.
- Esse possono, in primo luogo, scrivere alle società sospettate di agire in violazione della legge e chiedere loro di esprimersi sulle accuse.
- Le Autorità hanno poi il potere di stabilire concrete misure a cui le società debbono conformarsi servendosi, tra l'altro, di atti amministrativi che descrivono quali condizioni devono essere soddisfatte per consentire l'elaborazione e il trasferimento di dati.
- Nei casi più gravi le Autorità statali possono anche imporre un divieto assoluto di raccolta, elaborazione o uso di determinati dati.
- Le società possono inoltre essere multate.

53- Regno Unito

- Il ***Information Commissioner Office*** **(ICO)** ha il potere di emettere sanzioni pecuniarie fino a £ 500.000 nei confronti delle organizzazioni colpevoli di una grave violazione del *Data Protection Act* britannico.
- Una multa può essere inflitta solo se l'ICO ritiene che la violazione sia suscettibile di causare danni rilevanti o disagio agli interessati e se il data controller sapeva o avrebbe dovuto sapere che la violazione sarebbe avvenuta e avrebbe probabilmente causato danni o disagi notevoli.
- Le società nei cui confronti sono emesse le sanzioni pecuniarie hanno diritto di ricorso, ma nei casi in cui siano costrette a pagare e non lo facciano entro i termini prescritti, l'ICO può chiedere un decreto ingiuntivo alla **High Court** o alla **County Court**, al fine di recuperare le multe non pagate.
- Se l'ICO ritiene che una sanzione pecuniaria non sia appropriata, può servirsi di una serie di altri strumenti nel tentativo di garantire che le società coinvolte rispettino la legge.
- L'ICO può emettere avvisi informativi vincolanti per le imprese per costringerle a fornire alcune informazioni rilevanti ai fini delle indagini.

54- Il quadro costituzionale dell'UE

- Il quadro costituzionale dell'Unione europea, come modificato dal Trattato di Lisbona (2009), riconosce la **protezione dei dati personali come diritto fondamentale in sé** (rif. Carta dei diritti fondamentali, Art. 8; Art. 16 TFUE), indipendente dal più tradizionale **rispetto della vita privata e familiare**, come previsto dall'art. 7 della Carta (si v. inoltre, CEDU, Art . 8).
- Questi sviluppi sono stati rafforzati dalla **giurisprudenza della Corte europea dei diritti dell'uomo** *ex* Art . 8 CEDU (2000 e 2007) e rafforzati da parte della **Corte di giustizia europea** (2003) .

55- Il quadro costituzionale dell'UE

- La UE tende a vedere la **riservatezza dei dati come un diritto fondamentale** **meritevole di rigorose e complete garanzie legislative.**
- Parte di tali garanzie sono rappresentate dall'istituzione di autorità di regolamentazione indipendenti (le cd. "autorità per la protezione dei dati") aventi competenza piena in materia di tutela della riservatezza dei dati.
- Il quadro normativo tracciato dalla **direttiva 95/46** impone alle suddette autorità di operare in stretta collaborazione tra loro, rafforzando così il loro impatto pratico.

56- Le norme sulla protezione dei dati

- Gli obblighi di legge imposti al titolare del trattamento dei dati sono anche in gran parte posti al riparo da eventuali modifiche che intervengano su base contrattuale.
- Mentre la **direttiva sulla protezione dei dati dell'UE** prevede che vi sia spazio per la previsione di un'elaborazione dei dati in base al **consenso della persona interessata** (vedi art. 7(a) e 8(2)(a)), al contrario i meccanismi di consenso non permettono ai soggetti interessati di stipulare un accordo che consenta a un titolare del trattamento dei dati di derogare alle sue funzioni minime ai sensi, per esempio, dell'art. 6 ("principi relativi alla qualità dei dati") e art . 12 ("diritti di accesso").
- Il **regime normativo degli Stati Uniti** permette invece alla libertà contrattuale e ai meccanismi di mercato di impattare con grande libertà nella fissazione degli standard circa la riservatezza dei dati. Esso permette un notevole grado di "*contractual override*" degli interessi relativi alla *privacy* dei soggetti interessati.

57- Le garanzie legislative per la *privacy* dei dati

- **Le garanzie legislative previste dalla normazione statunitense per la riservatezza dei dati sono generalmente meno severe che in Europa**.
- Per esempio, negli **Stati Uniti** la legislazione si astiene dall'imporre restrizioni relative alla *privacy* in materia di esportazione dei dati personali verso altri paesi. I meccanismi di sorveglianza e di esecuzione concernenti la *privacy* dei dati sono anche molto meno sviluppati rispetto ai corrispettivi schemi attuati in Europa. **Non vi è alcuna autorità di regolamentazione federale** avente un mandato e poteri simili a quelli delle autorità europee per la protezione dei dati. In generale, il rispetto dei diritti di riservatezza dei dati è garantito attraverso il contenzioso in sede giudiziaria.
- Le misure legislative proposte in materia di solito incontrano una forte opposizione da parte dei gruppi di interesse del settore.

58- Stati Uniti e UE

- Le norme statunitensi ed europee in materia di *privacy* dei dati si basano su un insieme di principi sostanzialmente simili per garantire la protezione dei dati personali.
- Questi principi sono stati redatti nei primi anni ’70 da comitati di esperti che hanno lavorato contemporaneamente, ma indipendentemente l'uno dall'altro.
- Il **comitato di esperti del Consiglio d'Europa** che ha elaborato la Convenzione del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale collaborò con la **Commissione di esperti incaricata di redigere le linee guida OCSE** del 1980 sulla protezione della vita privata e dei flussi transfrontalieri di dati personali.

59- L'approccio giuridico degli Stati Uniti e dell'UE

- Nel caso *Sorrell v IMS Health*, Inc., la Corte Suprema degli Stati Uniti (2011) ha annullato una legge dello stato del Vermont che limitava la possibilità per le società farmaceutiche di acquistare le prescrizioni mediche senza il consenso dei medici, sulla base del fatto che la legge indebitamente violava la libertà di espressione (*i.e.* il **Primo Emendamento del *Bill of Rights* della Costituzione degli Stati Uniti**).
- Questo è un esempio della forte enfasi sulla libertà di espressione da parte del sistema legale statunitense.
- Secondo la legge degli **Stati Uniti** il trattamento dei dati personali è generalmente consentito.

60- L'approccio giuridico degli Stati Uniti e dell'UE (2)

- Al contrario, ai sensi del **diritto UE**, tale trattamento è vietato se non ha un solido ancoraggio normativo (cfr. in particolare gli artt. 7 e 8 della direttiva sulla protezione dei dati).
- Allo stesso modo, la **giurisprudenza della Corte europea dei diritti dell'uomo** ritiene che la semplice memorizzazione dei dati personali (anche se senza il consenso o la conoscenza della persona interessata) può costituire una interferenza con il diritto al rispetto della vita privata ai sensi dell'art. 8(1) CEDU, anche se non vi è alcuna prova che i dati siano utilizzati a scapito della persona interessata o dell'utilizzo degli stessi (CEDU 2000).

61- La riforma della Commissione europea delle norme sulla protezione dei dati

- **Obiettivo: aggiornare e modernizzare il quadro normativo.**
- L'iniziativa è il risultato di un ampio lavoro e di consultazioni pubbliche che durano da più di due anni.
- Le proposte della CE (presentate nel gennaio 2012 e ancora in corso) includono:

  1. una "**Communication policy**" che definisce gli obiettivi della Commissione,

  2. un **progetto di regolamento** che stabilisce un quadro comunitario generale per la protezione dei dati, in sostituzione della direttiva 95/46/CE,

  3. un **progetto di direttiva** sulla protezione dei dati personali trattati a fini di prevenzione, individuazione, indagine e perseguimento dei reati e delle connesse attività giudiziarie.

62- Un quadro normativo per la protezione dei dati più coerente e una migliore applicazione delle norme

- Il **progresso tecnologico** (ad es. Internet, i *social network* e i dispositivi mobili) e la **globalizzazione** (ad es. l'aumento di flussi transnazionali di condivisione dei dati) hanno profondamente cambiato il modo in cui i dati personali vengono raccolti, resi accessibili ed utilizzati (si pensi al *profiling* dei consumatori e al monitoraggio, la pubblicità comportamentale *on-line*, l'*outsourcing* dei dati e il *cloud computing*).
- Inoltre, i 28 Stati membri dell'UE hanno applicato le norme del 1995 in modo diverso. Di conseguenza, la CE ritiene che sia giunto il momento di **elaborare un quadro normativo più forte e più coerente per la protezione dei dati nell'UE che garantisca una migliore applicazione della legge**.

63- Un regolamento invece di una direttiva

- **La direttiva 95/46/CE sarà sostituita da un regolamento basato sull'art. 16 del TFUE**.
- Un regolamento è considerato "*lo strumento giuridico più appropriato per definire un livello comune di protezione dei dati in tutta l'Unione. L'applicabilità diretta di un regolamento ridurrà la frammentazione giuridica e fornirà maggiore certezza del diritto attraverso l'introduzione di un insieme armonizzato di regole di base*".
- Questa scelta è già stata molto criticata da un certo numero di parti interessate, essendo il regolamento considerato troppo invadente e prescrittivo rispetto ad una direttiva, che per sua natura è invece più flessibile. Inoltre, sembra che vi sia una mancanza di coerenza tra i vari strumenti nel nuovo pacchetto di protezione dei dati della CE, nonché rispetto alla **direttiva 2002/58/CE sulla *e-privacy*** del pacchetto Telecom, come modificato nel 2009.

64- Il diverso approccio della UE e del Consiglio d'Europa

- Nel marzo 2012 **il Consiglio d'Europa ha presentato le sue proposte d'aggiornamento della Convenzione n. 108 sulla tutela dei dati personali**.
- Anche se la UE e il Consiglio d'Europa condividono le stesse preoccupazioni, i loro approcci sono leggermente diversi.
- La Convenzione, che si pone come un potenziale standard universale e uno strumento chiave vincolante a livello globale, è meno prescrittiva e più focalizzata sui diritti umani. Tuttavia, la sua coerenza e compatibilità rispetto al quadro normativo comunitario è uno degli obiettivi fondamentali perseguiti dal Consiglio d'Europa.
- In generale, nella riforma della CE permangono ancora la struttura fondamentale e i principi generali e i concetti chiave della direttiva 95/46/EC4.
- La Commissione ha formulato una serie di proposte molto ambiziose per chiarire e migliorare il quadro normativo attuale e per garantirne un'efficace applicazione.

65- Un quadro normativo adeguato ed equilibrato

- **Obiettivo: garantire, in modo equilibrato, la *privacy* e la protezione dei dati, nonché la crescita economica, l'innovazione e la creazione di posti di lavoro**.
- Le **competenze della Commissione vengono fortemente rafforzate** attraverso l'adozione di "misure di esecuzione" e "atti delegati" che le assicurano la possibilità di definire in un secondo momento le regole specifiche di alcuni settori d'intervento, tra cui il diritto all'oblio e l'elaborazione dei dati personali dei minori.

66- Un quadro normativo adeguato ed equilibrato (2)

- L'**approccio di UE e USA** è **molto diverso** in termini di protezione dei dati e *privacy*. Mentre in Europa la protezione dei dati è riconosciuta come un diritto fondamentale sancito nei testi costituzionali, l'approccio degli Stati Uniti è più focalizzato sul fine commerciale e il diritto dei consumatori. Tuttavia sussistono numerosi **punti di convergenza** tra i due modelli per quanto riguarda il rafforzamento dei diritti degli utenti *on-line*, la necessità di aumentare l'armonizzazione delle leggi e dei regolamenti sulla privacy, migliorandone l'esecuzione e favorendo la cooperazione.

67- I cambiamenti essenziali nel progetto di regolamento

- In base al nuovo regolamento, ci sarà **solo un insieme di norme sulla protezione dei dati in tutta l'UE** e una sola autorità per la protezione dei dati sarà responsabile (secondo il modello "***one-stop-shop***") per una società che opera in diversi paesi: l'autorità nazionale dello Stato membro in cui la società ha la propria sede principale.
- L'estensione del **campo di applicazione territoriale**. Le norme Ue si applicheranno anche ai dati personali trattati all'estero da imprese che sono attive sul mercato unico e offrono servizi ai cittadini dell'Unione.
- Facilitazione dei **trasferimenti internazionali di dati**. In linea di principio, qualsiasi trasferimento di dati è oggetto di una **decisione della Commissione** sul fatto che il terzo in questione assicuri un "**livello di protezione adeguato**".

68- La responsabilità dei titolari del trattamento dei dati e dei responsabili dei dati

- **La responsabilità dei titolari del trattamento dei dati e dei responsabili dei dati sono aumentate.**
- La nomina di un responsabile della protezione dei dati per le aziende con oltre 250 dipendenti, la valutazione dei rischi di protezione dei dati e dei principi di trasparenza, di "*privacy by default*" e "*privacy by design*" (misure di salvaguardia da prevedere nei prodotti e servizi fin dalle prime fasi di sviluppo) per garantire che gli individui siano informati in modo facilmente comprensibile su come saranno trattati i loro dati .
- Un obbligo generale di **notifica della violazione di dati**: tutte le "violazioni di dati personali" (i.e. in caso di perdita, furto o *hacking* di dati personali): imprese e organizzazioni ovranno comunicare quanto prima, possibilmente entro 24 ore, alle autorità nazionali di controllo i casi di grave violazione dei dati.

69- I principali cambiamenti nel progetto di regolamento

- **I diritti delle persone interessate risultano rafforzati**. Il progetto di regolamento propone di fornire agli individui un maggior controllo sui propri dati personali attraverso disposizioni che trattano specificamente le nuove forme di media come i *social network*.
- **Il consenso degli individui al trattamento dei propri dati personali deve essere "esplicito"** (cioè deve essere manifestato da un'azione affermativa o da dichiarazione), oltre che "libero, specifico e informato", e revocabile in qualsiasi momento;
- L'introduzione del **diritto all'oblio**, permetterà di gestire meglio i rischi connessi alla protezione dei dati online: chiunque potrà cancellare i propri dati se non sussistono motivi legittimi per mantenerli.
- Un nuovo **diritto alla portabilità dei dati:** agevolazione del trasferimento dei dati da un fornitore di servizi a un altro, il che comporterà un miglioramento della concorrenza tra i servizi.

70- L'applicazione delle norme

- Il **rafforzamento dei poteri e degli strumenti delle autorità nazionali di protezione dei dati** ha giovato al fine dell'applicazione e del consolidamento delle norme in materia a livello europeo.
- Le autorità nazionali di protezione dei dati possono, tra l'altro, imporre **sanzioni amministrative** efficaci e deterrenti in caso di violazione delle norme sulla protezione dei dati. Il progetto di regolamento stabilisce infatti un regime di intervento a più livelli.
- La multa massima che un regolatore nazionale può imporre per **gravi violazioni** del regolamento (ossia in caso di omissione della designazione del responsabile della protezione dei dati o in mancanza della notifica a un regolatore di una violazione della sicurezza) è di un **milione di euro o una somma pari al 2 % del fatturato annuale di una impresa.** Vi è anche il problema di migliorare la **cooperazione tra le autorità di vigilanza nazionali** (con strumenti di assistenza reciproca e operazioni congiunte) nonché i meccanismi di coerenza attraverso l'istituzione di un Comitato europeo per la protezione dei dati.

71- La modernizzazione della Convenzione COE n. 108

- Il processo di modernizzazione della Convenzione n. 108 ha avuto inizio in occasione della 5° edizione della Giornata della protezione dei dati (**28 gennaio 2011**), quando il Segretario Generale del Consiglio d'Europa ha lanciato una **consultazione pubblica** volta a raccogliere le istanze dei governi, della società civile e del settore privato.
- In seguito sono state ricevute **50 risposte** da parte di tutti i soggetti interessati: governi, autorità di protezione dei dati, ONG, settore privato, associazioni professionali, inclusi soggetti non europei, principalmente provenienti dalle Americhe e dall'Africa. Tali risposte sono state analizzate e recepite nelle proposte di modernizzazione.
- La modernizzazione e la promozione della Convenzione n. 108 ha rappresentato una **priorità** nel corso del biennio 2012-2013 appena conclusosi.

72- Gli obiettivi

- Il **processo di revisione persegue due obiettivi principali**:
- 1. Affrontare le sfide per la *privacy* derivanti dall'uso delle nuove ICT;
- 2. Rafforzare il meccanismo di follow-up della Convenzione. Come chiaramente emerso dalla consultazione pubblica, vi è un ampio consenso sugli obiettivi da perseguire:

  a) garantire il carattere generale e tecnologicamente neutrale delle disposizioni della Convenzione con testi settoriali più dettagliati e strumenti non vincolanti (pareri e raccomandazioni);

  b) assicurare la coerenza e la compatibilità con il quadro giuridico dell'Unione europea;

  c) riaffermare il potenziale della Convenzione quale standard universale avente carattere aperto.

73- Le modifiche principali

- **Articolo 1 - Oggetto e scopo**

Si propone di fare riferimento, oltre che al diritto alla *privacy*, al **diritto alla protezione dei dati personali**, che ha acquisito un significato autonomo nel corso degli ultimi 30 anni. Il riferimento al concetto di competenza e non di "territorio" al fine di definire l'ambito geografico di applicazione della Convenzione è in linea con il diritto internazionale pubblico.

74- Modifiche fondamentali (2)

- **Articolo 3 - Ambito di applicazione**

Emerge chiaramente dalle risposte alla consultazione che è consigliabile mantenere l'**approccio globale** della Convenzione, che trova applicazione nel settore pubblico e privato.

Si propone di applicare la Convenzione ad ogni trattamento dati che sia soggetto alla competenza di una parte. Invece, la questione del trattamento derivante da attività e servizi offerti alle persone, effettuati dai titolari del trattamento che non sono soggetti alla competenza di una parte, resta da esaminare, in particolare alla luce delle sentenze della Corte di giustizia dell'Unione europea nei casi ***Lindqvist*** (6 novembre 2003) e ***Pammer/Alpenhof*** (7 dicembre 2010), e rispetto alle principali decisioni dei giudici nazionali in materia di competenza *on-line*. Appare necessario includere un'eccezione per il trattamento dei dati familiari. I ***social network***, ***blog*** etc. richiedono un'attenzione specifica. Si propone infine di applicare pienamente la Convenzione ogni volta che i dati personali siano accessibili a soggetti terzi rispetto alla sfera personale o domestica.

75- Modifiche fondamentali (3)

- **Articolo 5 - Legittimità del trattamento dei dati e qualità dei dati**

Si prevede di includere espressamente **il principio di proporzionalità**, a seguito della giurisprudenza della Corte europea dei diritti dell'uomo, che richiede un giusto equilibrio tra gli interessi concorrenti pubblici e privati (*S e Marper c. Regno Unito* [2008], 118). La versione originale dell'art.5 non menzionava il "consenso esplicito". Invece ora si propone di richiedere un **consenso specifico, libero e informato**, che prevalga sugli interessi legittimi e sugli obblighi legislativi o aventi fonte contrattuale come condizione della liceità del trattamento.

- **Articolo 6 - Trattamento dei dati sensibili**

Si propone di rivedere l'attuale definizione al fine di includere anche i dati relativi alla salute, alla genetica e ai dati biometrici.

- **Articolo 7 - Sicurezza dei dati**

La sicurezza interessa sia i dati sia il loro trattamento. Le garanzie saranno rafforzate richiedendo la segnalazione di violazioni della sicurezza, distinguendo tra obblighi dei titolari e dei responsabili del trattamento.

76- Modifiche fondamentali (4)

- **Articolo 8 – I diritti della persona interessata**

La proposta non prevede l'inclusione esplicita di un **diritto all'oblio**. Si è infatti ritenuto che il combinato disposto delle garanzie esistenti (in particolare l'art 5 lett.e (durata della memorizzazione dei dati), e l'art 8 lett.c (diritto di rettifica o cancellazione dei dati)) e del diritto di opposizione garantisse una protezione adeguata.

- **Articolo 8-*bis* - Ulteriori misure per il titolare del trattamento**

Questo nuovo provvedimento recepisce il principio della responsabilità per le misure concrete per il titolare del trattamento, come l'obbligo in casi determinati di svolgere **un'analisi dei rischi della protezione dei dati**, per progettare il trattamento in modo tale da ridurre al minimo il rischio o stabilire meccanismi interni per dimostrare la conformità del trattamento alla legge applicabile. L'adeguatezza di tali requisiti dipenderà dalle dimensioni della società interessata.

77- Modifiche fondamentali (5)

- **Articolo 9 - Eccezioni e limitazioni**

A parte alcune modifiche terminologiche proposte, le deroghe ai requisiti di alcune disposizioni sono necessarie per conciliare il diritto alla protezione dei dati personali con la **libertà di espressione e di informazione**. Si propone inoltre una nuova eccezione per i flussi di dati a tutela della libertà di espressione e di informazione.

- **Articolo 12 - I flussi transfrontalieri**

La questione del flusso transfrontaliero dei dati è fondamentale nel processo di modernizzazione. Le disposizioni proposte impattano sulle disposizioni esistenti in materia di flussi transfrontalieri di dati sia nella Convenzione sia nell'art. 2 del protocollo addizionale del 2001 (sul trasferimento di dati a Stati che non sono parti).

78- Modifiche fondamentali (6)

- **Il nuovo capitolo 3-*bis*: le autorità di vigilanza**

Un nuovo capitolo integrerà le disposizioni finora contenute nel protocollo aggiuntivo del 2001 alla Convenzione, rafforzando l'**indipendenza e i poteri delle autorità di vigilanza** (ad es. prevedendo un'iniziativa *ex officio*, l'intervento dinanzi al giudice per i procedimenti già in corso, il coordinamento delle indagini nei casi transfrontalieri).

79- Osservazioni generali

- "**Obiettivi**" e "**orientamenti generali**": la natura generale e tecnologicamente neutrale della Convenzione; la coerenza e la compatibilità con il quadro giuridico dell'UE; il carattere universale e aperto della Convenzione.
- Tra le **importanti questioni** sollevate nella Convenzione, che possono avere un impatto importante sulle attività dei media, e in particolare nel settore *on-line*, vi sono: l'eccezione per la libertà di espressione (o "esenzione giornalistica"), gli obblighi dei titolari del trattamento e i trasferimenti internazionali di dati.
- L'inclusione di una deroga esplicita per "la libertà di espressione e di informazione" nel preambolo e nell'art. 9(1)(b) della Convenzione.

80- Compatibilità con il quadro giuridico dell'UE

- Varie proposte sembrano essere ben **equilibrate e proporzionate** rispetto alle disposizioni del progetto di regolamento CE, per esempio, il riferimento esplicito al principio di proporzionalità nel contesto della legittimità del trattamento dei dati (art. 5); il riferimento a una notifica delle violazioni dei dati "senza indugio" di cui all'art. 7,2; il fatto che verranno previste misure aggiuntive (ad esempio la protezione dei dati di valutazione dei rischi) per il titolare del trattamento a seconda, ad esempio, della dimensione della società interessata (art. 8-*bis*) e il fatto che spetti a ciascuna delle parti di stabilire sanzioni e rimedi adeguati (art. 10).