UNINDUSTRIA

Roma, 25 maggio 2017

Nuove regole, adempimenti e responsabilità, fra Regolamento Privacy e Direttiva NIS

Maurizio Mensi

Scuola Nazionale dell'Amministrazione - Luiss Guido Carli

Responsabile @LawLab Luiss

SOMMARIO

1. Un quadro normativo nuovo e in evoluzione, a vari livelli
2. Il "pacchetto Privacy"
3. Il Regolamento GDPR e le sue innovazioni
4. Modifiche organizzative e gestionali per imprese e PA
5. La Direttiva NIS del 2016

LA STRATEGIA E LE REGOLE UE

- **2006 –Strategia per una società dell'informazione sicura**
- **2013 – Strategia in tema di Cybersecurity**
- ***Europe Strategy* 2020** - Agenda Digitale, Pilastro III: rafforzare fiducia e sicurezza
- **Comunicazione 20 giugno 2014 (strategia di sicurezza interna)**

Concetto di «**sicurezza nazionale**» - Standard di riferimento condivisi

- **Convenzione del Consiglio d'Europa sul *Cybercrime*** (Budapest, 23 novembre 2001)
- **Dir. 2008/114/CE** – *Network* fisico (energia e trasporti) - **Dir. 2013/40/UE**

Attacchi contro i sistemi di informazione – Standard minimi per la definizione dei reati - **Direttiva 2002/58 *e-privacy***

- **La revisione della Convenzione COE n. 108/1981**
- **Il Pacchetto Privacy (Regolamento 2016/679 e Direttiva *Enforcement*)**
- **La Direttiva NIS 2016/1148– *Network and Information Security***

Settore pubblico e privato - 5 elementi: nuova strategia nazionale – rete di cooperazione - requisiti di sicurezza – standards – *enforcement*

IL QUADRO DI RIFERIMENTO IN ITALIA

- **2010-** Relazione sulla politica di informazione per la sicurezza
- **Evoluzione normativa** – La sicurezza della Repubblica (**leggi n. 801/1977 - n. 124/2007 – n. 133/2012**)
- **DPCM 24 gennaio 2013** – Quadro strategico nazionale e Piano nazionale per la protezione cibernetica e la sicurezza informatica (19 febbraio 2014) - Il Tavolo Tecnico Cyber (TTC)
- **DPCM 17 febbraio 2017** sulla nuova architettura per la protezione dello spazio cibernetico nazionale

Il CERT (*Computer Emergency Response Team*) nazionale – **Il ruolo di AGID (legge n. 83/2012)**

- **Il *cybercrime* e gli strumenti normativi**
- **Legge 31 luglio 2005 n. 155** sulla prevenzione dei reati terroristici
- **La legge «antiterrorismo» 17 aprile 2015, 43**
- **Codice Privacy, d.lgs. 30 giugno 2003, n. 196**
- **La violazione dei dati personali** - La procedura - *Data Breach Notification* (Dir. 2002/58, Dir. 136 e 140 del 2009 – D. Lgs n. 196/2003, Codice Privacy – Linee guida del Garante Privacy - Delibera 4/4/2013 – Reg. UE n. 611/2013 – **Reg. 2016/679**).

UN QUADRO ADEGUATO E TEMPESTIVO ?

La prima regola della cybersicurezza, per imprese e cittadini / consumatori, é il rispetto delle regole

- Quali ? Stabilite da chi ? Complete e aggiornate ?
- **Cantiere normativo in corso**, a livello internazionale, europeo e nazionale – singolare congiuntura

Codice Privacy (d.lgs. n. 196 del 2003), ancora applicabile in toto dopo l'entrata in vigore del Regolamento europeo ?

- Sfera pubblica e privata …
- Concetto di **sicurezza nazionale** (tema di competenza nazionale - considerato 16 del Reg.).
- **I dati come bene essenziale e materia prima, al centro di una battaglia quotidiana**

LA DIRETTIVA NIS

- **Riconoscimento di un insufficiente livello di protezione.**
- Rischio per il mercato interno– sistemi interconnessi –incidenti superano confini nazionali – interventi regolamentari degli SM non coordinati dannosi – alcuni settori chiave a supporto del mercato interno: **banche – borse valori – energia (generazione, trasmissione e distribuzione), trasporti, salute –**
- **operatori di servizi essenziali e fornitori di servizi digitali.**
- Le attività riguardanti **la sicurezza nazionale** sono di competenza nazionale (considerato 16 del Reg.).
- **Lacune nell'attuale assetto regolamentare – Data controllers** (banche, ospedali) sono costretti a porre in essere misure di sicurezza proporzionate al livello di rischio che fronteggiano, ma sono tenute a notificare le violazioni di sicurezza soltanto nel caso in cui siano compromessi dati personali.
- **La Direttiva 2008/114 sulle Infrastrutture critiche europee** riguarda soltanto trasporti ed energia e non pone alcun obbligo agli operatori di segnalare danni ai sistemi di sicurezza o di cooperare.

I PUNTI CHIAVE

L'obiettivo della **Direttiva 2016/1148** è raggiungere un **livello elevato di sicurezza** dei sistemi, delle reti e delle informazioni comune a tutti i Paesi membri dell'UE.

I **tre punti** chiave della direttiva NIS sono:

1. Migliorare le capacità di **cyber security** dei singoli Stati dell'Unione;
2. Aumentare il livello di **cooperazione tra gli Stati dell'Unione**;
3. **Obbligo di gestione dei rischi** e di comunicare gli incidenti di una certa entità da parte degli **operatori di servizi essenziali e dei fornitori di servizi digitali.**

- La direttiva lascia impregiudicata la possibilità, per ciascuno Stato membro, di adottare le misure necessarie per assicurare la tutela degli interessi essenziali della sua sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati.

I SOGGETTI RIGUARDATI

- La cooperazione tra i vari enti dei singoli Stati membri è un aspetto fondamentale della direttiva NIS. Proprio per questo è stato stabilito **un gruppo di cooperazione** che faciliti i rapporti tra gli Stati membri e che aumenti la fiducia. Questo gruppo di cooperazione sarà composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA (European Union for Network and Information Security Agency).

A CHI SI APPLICA ? Gli operatori dei servizi essenziali e i fornitori di servizi digitali.

- **Gli operatori di servizi essenziali** sono aziende pubbliche o private che hanno un ruolo importante per la società e l'economia. Sono identificati direttamente da ogni Stato membro, all'interno dei seguenti ambiti: **energia, trasporti, banche e società finanziarie, salute, acqua ed infrastrutture digitali.**
- **I criteri per l'inclusione nella lista** sono: l'essenzialità del servizio offerto per il mantenimento di attività critiche in ambito economico e sociale; il servizio dipende da sistemi informatici; se l'incidente di sicurezza rischia di avere effetti gravi e significativi sulla fornitura di un servizio essenziale.
- La Direttiva obbligherà queste entità a dotarsi di **misure di sicurezza appropriate** e di notificare all'autorità nazionale competente gravi incidenti di sicurezza secondo parametri di numero di utenti coinvolti, durata dell'incidente e diffusione geografica. **Le misure di sicurezza richieste comprendono: prevenzione dei rischi; garantire la sicurezza dei sistemi, delle reti e delle informazioni; capacità di gestire gli incidenti.**
- **I fornitori di servizi digitali** sono identificati nei motori di ricerca, gli operatori del mercato on line e di servizi cloud.

CRONOLOGIA

- **6 luglio 2016**: adozione.
- **agosto 2016:** entrata in vigore.
- **agosto 2017:** i fornitori di servizi digitali devono adottare i requisiti minimi di sicurezza e di notifica degli incidenti.
- **maggio 2018:** trasposizione all'interno degli ordinamenti nazionali.
- **novembre 2018:** ogni Stato membro dovrà identificare gli operatori di servizi essenziali.
- **2019:** la Commissione europea valuterà la coerenza dell'identificazione degli operatori di servizi essenziali da parte degli Stati membri.
- **2021:** sará riesaminato il funzionamento della direttiva con particolare attenzione alla cooperazione strategica e operativa degli Stati e la sua applicazione.

STRATEGIA NAZIONALE

- Ogni Stato infatti dovrà dotarsi di una **strategia nazionale** di cyber security che definisca gli obiettivi strategici, le politiche adeguate e le misure di regolamentazione. Tra gli aspetti che una strategia nazionale dovrebbe includere vengono citati gli obiettivi strategici, le priorità nazionali, la *governance*, l'individuazione di misure proattive, di risposta e di *recovery*; sensibilizzazione, formazione ed istruzione; incentivazione della cooperazione tra settore pubblico e settore privato; lista degli attori coinvolti nella attuazione della strategia.
- La Direttiva richiede agli Stati di designare **una o più autorità competenti** per il controllo dell'applicazione della direttiva stessa a livello nazionale **(Authority).** Un singolo punto di contatto dovrà essere designato da ognuno degli Stati membri, con il compito di assicurare la **cooperazione internazionale** e di collegarsi con gli altri Stati attraverso meccanismi di cooperazione identificati della direttiva stessa.
- Ogni Stato dovrà infine designare uno o più **CSIRT (Computer Security Incident Response Team)** responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti. Dovranno inoltre fornire analisi sui rischi e incidenti e aumentare il grado di consapevolezza. Fondamentale anche per i CSIRT è la **cooperazione internazionale e l'information sharing**

CULTURA DELLA SICUREZZA

- La direttiva si propone di sviluppare **una cultura della sicurezza e della gestione dei rischi, garantendo lo scambio regolare di informazioni tra settore privato e pubblico.**
- La notifica degli eventi critici al riguardo è essenziale: le aziende tendono spesso a non divulgare o minimizzare gli incidenti per non intaccare la fiducia dei consumatori verso le imprese detentrici di dati sensibili.
- La direttiva affida una grande responsabilità ai **fornitori di servizi essenziali.**
- Occorre poi ricordare che, per esempio, anche se una società di servizi finanziari, assicurativi o sanitari delega i servizi di cloud computing a terzi, è su di essa che ricade **la principale responsabilità in caso di violazione di dati o attacco informatico.**

PRIVACY - L'INTERVENTO NORMATIVO UE

25 gennaio 2012: la Commissione europea propone la **riforma della normativa UE in materia di protezione dei dati** per:

1. ampliare le opportunità delle aziende che desiderano investire nel mercato interno all'Unione Europea, assicurando un livello elevato di protezione dei dati degli individui,
2. incrementare e rendere più sicuri i trasferimenti di informazioni tra Stati membri e le autorità giudiziarie per circoscrivere i fenomeni di criminalità informatica,
3. aprire la strada verso una maggiore armonizzazione della normativa sulla protezione di dati in Europa mettendo fine alla frammentazione che caratterizza il quadro normativo attuale.

27 aprile 2016: approvato il ***Pacchetto Privacy***:

A. **Regolamento 2016/679 c**he stabilisce un quadro generale dell'Unione per la protezione dei dati, che sostituisce la **Dir. 95/46.**
B. **Direttiva 2016/680** sulla protezione delle persone fisiche con riguardo al trattamento dei dati ai fini di prevenzione, indagine, accertamento o perseguimento dei reati e nell'ambito delle connesse attività giudiziarie.

UN REGOLAMENTO AL POSTO DI UNA DIRETTIVA

- Il **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***".

LA TEMPISTICA PER L'ENTRATA IN VIGORE

4 maggio 2016: pubblicazione del **Regolamento** nella Gazzetta UE.

A partire dal ventesimo giorno dalla pubblicazione (24 maggio), gli SM hanno **due anni di tempo** per allineare la normativa nazionale alle nuove prescrizioni introdotte dal Regolamento, che diventerà definitivamente **applicabile** in tutto il territorio UE a partire dal **25 maggio 2018**.

Per quel che concerne la **Direttiva**, gli Stati membri avranno due anni per recepire con apposite norme le sue disposizioni all'interno dell'ordinamento nazionale.

LE PRINCIPALI NOVITÀ - AMBITO DI APPLICAZIONE TERRITORIALE

La **Direttiva 95/46** prevede che la disciplina in materia di tutela di dati personali trovi applicazione, attraverso la normativa nazionale, quando **il trattamento di dati personali sia effettuato "*nel contesto delle attività di uno stabilimento del titolare situato nell'UE*".**

Invece il **Regolamento** ha un diverso **ambito di applicazione in quanto** estende l'ambito di applicazione anche a **titolari e responsabili di trattamento** ("Titolari" e "Responsabili") **non residenti nell'UE.**

Si applica "**indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione**" e impone l'applicazione delle sue regole anche a **titolari e responsabili non stabiliti nell'UE** che:

(i) **trattino dati personali di persone fisiche che si trovano nell'UE** quando il trattamento sia in relazione a offerte di beni e servizi, indipendentemente dal fatto che sia richiesto o meno un pagamento o

(ii) **effettuino attività di monitoraggio sul comportamento di persone fisiche che si trovano nell'UE** nella misura in cui tale comportamento avvenga nell'UE.

Seguito della sentenza **Google Spain (2014):** la normativa europea in materia di tutela dei dati personali si applica anche a casi in cui i titolari sono soggetti non europei e i dati sono trattati principalmente fuori dall'Europa.

NUOVI OBBLIGHI E RESPONSABILITÀ

Il Regolamento ridefinisce le figure di **titolare e responsabile** attribuendo loro obblighi ulteriori rispetto a quanto previsto dalla Dir. 95/46 e dal Codice Privacy e rafforzando la loro **responsabilità** ("*accountability*", Artt. 24 e 32).

Il **titolare** ha un ruolo più proattivo e obblighi finalizzati non soltanto al formalistico rispetto delle regole, ma anche all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire l'applicazione effettiva dei trattamenti, anche sotto il profilo della sicurezza.

IL TRATTAMENTO DEI DATI

COSA CAMBIA ?

- Per i dati "sensibili" il consenso **DEVE** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – Art. 22)
- **NON** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili).
- Il titolare (art. 7.1) **DEVE** essere in grado di dimostrare che l'interessato ha prestato il **consenso a uno specifico trattamento.**
- Il **consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

COSA NON CAMBIA ?

- Il consenso **DEVE** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **NON** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).
- **DEVE** essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

IL TRATTAMENTO DEI DATI (2)

COSA FARE ?

- Il consenso raccolto precedentemente al **25 maggio 2018** resta valido se ha tutte le caratteristiche indicate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento.
- In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (Art. 7.2).
- **I soggetti pubblici** non devono, di regola, chiedere il consenso per il trattamento dei dati personali (considerando 43, Art. 9, Artt. 18, 20 Codice).

OBBLIGHI DI TRASPARENZA

Una sezione del Regolamento è dedicata alla **"Trasparenza"** (Sezione 1 del Capo III) e alle modalità di trattamento dei dati (Artt. 5 e 12).

Le informazioni all'interessato (la cd ***informativa)*** devono:

(i) essere rese con un **linguaggio semplice e chiaro, soprattutto nel caso di minori;**

(ii) avere sempre **forma scritta** (ferma la possibilità di utilizzare apposite modalità elettroniche). L'informativa in forma orale è ammessa solo quando ciò sia richiesto dall'interessato e l'identità di questi possa essere provata con altri mezzi;

(iii) Prevedere: (**a) il periodo di conservazione dei dati personali, (b) il diritto di proporre reclamo ad un'autorità di controllo, (c) l'intenzione del titolare di trasferire dati personali a un paese terzo.**

DIRITTO ALLA PORTABILITA'

- Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).
- **Non si applica ai trattamenti non automatizzati** (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "**forniti**" **dall'interessato** al titolare.
- Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

PRIVACY BY DESIGN E BY DEFAULT

Il regolamento pone con forza l'accento sulla **"responsabilizzazione" (accountability) di titolari e responsabili** – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (Artt. 23-25, e Capo IV).

Novità: viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati.

La ***PRIVACY BY DESIGN*** richiede che Il titolare adotti e attui misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati.

La ***PRIVACY BY DEFAULT*** presuppone invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

Giá presenti nel **Codice Privacy** (Artt. 3 e 11 lett. 3), richiamano i principi di minimizzazione e di necessità.

DATA BREACH

Attualmente solo i "**fornitori di servizi di comunicazione elettronica accessibili al pubblico**" hanno l'obbligo di comunicare l'avvenuta violazione di dati personali:

a) al Garante per la protezione dei dati personali e
b) in determinati casi, anche al contraente/cliente.

Il **Regolamento** (Artt. 33 e 34) estende tale obbligo di comunicazione a tutti i titolari e responsabili, quali che siano i trattamenti posti in essere.

LA PROCEDURA

Il responsabile **deve informare il titolare** senza ingiustificato ritardo della violazione e quest'ultimo deve notificare la violazione, a sua volta senza ingiustificato ritardo, **all'autorità di controllo (es. al Garante)** e, ove possibile, entro **72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone. Qualora la notifica non sia effettuata entro **72 ore**, deve essere fornita una motivata giustificazione.

La notifica deve contenere almeno, a titolo esemplificativo e non esaustivo:

(i) la descrizione della natura della violazione e, ove possibile, il numero degli interessati,

(ii) il contatto del responsabile della protezione dati o di altro punto di contatto per ottenere più informazioni,

(iii) la descrizione delle misure adottate o che si intende adottare per porre rimedio alla violazione dei dati.

È previsto inoltre un obbligo di comunicazione anche all'interessato, se la violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche.

ESCLUSIONE DALL'OBBLIGO DI NOTIFICA

E' escluso l'obbligo di notifica all'interessato nei casi seguenti:

(i) se il titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione,

(ii) se il titolare ha successivamente adottato misure atte a scoraggiare il sopraggiungere di un elevato rischio per i diritti degli interessati;

(iii) se tale comunicazione richiede sforzi sproporzionati (in tal caso si procede con una comunicazione pubblica tramite la quale gli interessati sono informati con analoga efficacia).

L'obiettivo è di consentire **all'autorità di controllo di attivarsi senza ritardo** in modo da valutare quale sia la gravità della violazione e quali misure imporre al titolare.

Mentre per la notifica all'autorità di controllo si richiede "**un rischio per i diritti e le libertà degli individui**", per la notifica all'interessato è necessario che **il rischio sia "elevato"**, quindi un livello di pericolo maggiore anche per evitare di suscitare inutili allarmismi per gli interessati a fronte di violazioni solo potenziali.

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (Art. 33, par. 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'Art. 32-bis, comma 7, del Codice. E' importante, pertanto, che i titolari di trattamento adottino le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Quando un determinato trattamento, tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità, presenta un **rischio elevato per i diritti e libertà delle persone fisiche**, il titolare deve effettuare una valutazione d'impatto dello stesso sulla protezione dei dati **("Valutazione d'impatto").**

L'autorità di controllo (es. il Garante) predispone e rende pubblico un elenco dei trattamenti che sono soggetti a valutazione d'impatto e quelli che invece non vi sono soggetti, comunicandoli al **Comitato europeo per la protezione dei dati.** La **valutazione d'impatto** (Art. 35) deve contenere:

(i) una descrizione dei trattamenti previsti e delle finalità del trattamento;

(ii) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

(iii) una valutazione per i rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi.

LA VALUTAZIONE D'IMPATTO

La **valutazione d'Impatto** è richiesta in particolare nei seguenti casi:

a) valutazione **sistematica e globale di aspetti personali relativi a persone fisiche**, basata su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono su tali persone fisiche;

b) **trattamento su larga scala di dati sensibili e giudiziari**;

c) **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.

È previsto che il titolare riveda **costantemente** la valutazione d'impatto.

REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

Il responsabile e il titolare devono tenere un **registro delle attività di trattamento in forma scritta**, anche in formato elettronico (Art. 30).

L'obbligo di tenuta dei registri non si applica tuttavia in linea di principio alle imprese o organizzazioni con meno di 250 dipendenti (con limitate eccezioni).

IL REGISTRO

- E' uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.
- La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, è opportuno che tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, si dotino di tale registro e, in ogni caso, effettuino un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.
- I contenuti del registro sono fissati all'Art. 30; tuttavia, nulla vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

MISURE DI SICUREZZA

Devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (Art. 32, par. 1); in questo senso, **la lista di cui al par. 1 dell'Art. 32 è una lista aperta e non esaustiva**.

Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** (Art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da Art. 32 del regolamento.

E' possibile utilizzare l'adesione a **specifici codici di condotta o a schemi di certificazione** per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di **linee-guida o buone prassi** sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'Art. 6, par. 1), lettere c) ed e) del regolamento) potranno restare in vigore (ex Art. 6, par. 2, Reg.) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex Artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

RESPONSABILE DELLA PROTEZIONE DATI

Il Regolamento individua un'ulteriore figura rispetto al Codice Privacy.

Il titolare o il responsabile devono designare un **responsabile della protezione dati - RPD** (Art. 37) qualora:

1) il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico;

2) le attività principali del titolare o del responsabile consistano in trattamenti che, per loro natura, campo di applicazione e/o finalità richiedano il controllo regolare e sistematico degli interessati su larga scala;

3) il titolare o il responsabile trattino dati sensibili o giudiziari.

Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: ***Data Protection Officer***) riflette l'approccio responsabilizzante che è proprio del regolamento (Art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile.

Non è un caso, infatti, che fra **i compiti del RPD** rientrino "**la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto** di cui all'Art. 35. La sua designazione è obbligatoria in alcuni casi (Art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura **(indipendenza, autorevolezza, competenze manageriali**: Artt. 38 e 39) *in* termini che il WP29 ha chiarito con linee-guida (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287)

I COMPITI DELL'RDP

L'RDP deve essere designato in base alla sua **professionalità** e, in particolare, alla sua **conoscenza della legislazione di protezione dei dati** ed è tenuto a:

1. informare e consigliare il titolare o il responsabile in merito agli obblighi derivanti dal Reg. e da altre disposizioni dell'UE;
2. verificare che il Reg. sia osservato;
3. fornire, se richiesto, un parere in merito alla valutazione d'Impatto;
4. cooperare con l'autorità di controllo.

DIRITTI DELL'INTERESSATO - DIRITTO ALL'OBLIO

Fino a oggi questo diritto era il risultato dell'elaborazione giurisprudenziale (il caso **Google Spain** della CGUE, 2014), delineato come il diritto dell'individuo ad essere "disindicizzato" dai risultati dei motori di ricerca o dai mezzi di informazione.

Il Reg. riconosce per la prima volta in diritto positivo il diritto all'oblio (Art. 17), attribuendo all'interessato il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i suoi dati personali:

(i) che non siano più necessari per le finalità per le quali sono stati raccolti;

(ii) quando abbia ritirato il consenso o si sia opposto al trattamento o il trattamento dei dati personali non sia altrimenti conforme al Regolamento.

Non sussiste il diritto all'oblio quando il trattamento è necessario per l'esercizio del **diritto alla libertà di espressione e di informazione o per l'adempimento di un obbligo legale**.

PORTABILITÀ DEI DATI

L'interessato ha il diritto (Art. 20) di:

(i) ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati che lo riguardano forniti al titolare;

(ii) trasmettere i propri dati (es. quelli relativi al proprio "profilo utente") da un titolare (es. un *social network*) ad un altro titolare, senza ostacoli da parte di colui al quale sono stati forniti in precedenza.

ARMONIZZAZIONE - ONE-STOP-SHOP

Sovente un medesimo trattamento di dati è operato dallo stesso titolare in più di un paese dell'UE, coinvolgendo cittadini europei di Stati diversi.

Per affrontare tale situazione, il Reg. individua **un'unica autorità di controllo** ("***Lead Authority***") identificata con riferimento al luogo dello stabilimento principale e/o unico del titolare o del responsabile, nel caso in cui questi ultimi effettuino trattamenti transfrontalieri.

Ciò al fine di evitare che violazioni delle medesime norme del Reg. possano essere oggetto di ricorsi decisi diversamente a seconda dell'autorità di controllo del Paese di riferimento.

In ogni caso è previsto un meccanismo per garantire cooperazione e assistenza reciproca fra le varie autorità eventualmente coinvolte.

TRASFERIMENTI INTERNAZIONALI DI DATI

- Un importante problema riguarda il **trasferimento internazionale di dati**.
- L'Art. 25 della Direttiva 95/46 **vieta i trasferimenti di dati personali** verso paesi che non garantiscono un livello adeguato di protezione. Vedasi Capo V, Artt. 44-50, Reg. 2016/679.
- 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.
- La UE riconosce anche **Svizzera, Canada, Argentina, Jersey, Guernsey e l'Isola di Man** come paesi aventi un livello adeguato di protezione dei dati.
- Nel 2000 la CE ha recepito tali principi (**Decisione *Safe Harbor***). Tuttavia i principi "*Safe Harbor*" sono stati bersaglio di molte critiche per quanto riguarda la loro applicazione e rispetto.
- Infatti è stato evidenziato come talora gli "**interessi economici strategici degli Stati Uniti**" si scontrassero con i principi "*Safe Harbor*".
- **La sentenza Schrems della CGUE (6 ottobre 2015)**
- **Il Privacy Shield (luglio 2016)**

TRASFERIMENTO INTERNAZIONALE DI DATI

- **Viene meno il requisito dell'autorizzazione nazionale** (Art. 45, par. 1, e Art. 46, par. 2). Ciò significa che il trasferimento verso un paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di **clausole contrattuali modello, debitamente adottate,** o di **norme vincolanti d'impresa** approvate attraverso la specifica procedura di cui all'art. 47 del Reg., potrà avere inizio senza attendere l'autorizzazione nazionale del Garante, a differenza di quanto attualmente previsto dall'art. 44 del Codice.
- Tuttavia, **l'autorizzazione del Garante** **sarà ancora necessaria** se un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi** stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.
- Il Reg. consente di ricorrere anche a **codici di condotta** ovvero a **schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'Art. 46. Ciò significa che i **titolari o i responsabili del trattamento stabiliti in un paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta** o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso paesi terzi, al fine di legittimare tali trasferimenti.
- **Tuttavia** (Art. 40, par. 3, e Art. 42, par. 2), tali titolari dovranno **assumere**, inoltre, **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati.

IL LEGISLATORE NAZIONALE

Il Regolamento (considerando 10 e 19) consente agli Stati membri di mantenere o introdurre previsioni più specifiche per adattare le disposizioni del Reg., soprattutto con riferimento al **trattamento di dati sensibili.**

In particolare gli Stati membri possono prevedere deroghe rispetto a quanto stabilito dal Reg. con riferimento ai trattamenti per scopi giornalistici, all'accesso del pubblico ai documenti ufficiali, al trattamento dei dati nell'ambito del rapporto di lavoro.

SANZIONI AMMINISTRATIVE

Il sistema sanzionatorio viene uniformato e rafforzato.

L'autorità di controllo viene dotata del potere di imporre **sanzioni amministrative** (Art. 83) per un importo pecuniario massimo predeterminato, tenendo conto, nella determinazione del *quantum*, di elementi quali: (i) la natura, la gravità e la durata della violazione, (ii) il carattere doloso o colposo della stessa, (ii) le misure adottate dal titolare).

Le sanzioni variano a seconda che si tratti di persona fisica o impresa.