Comune di Modena

Regione Emilia-Romagna

Forum Italiano per la Sicurezza Urbana

Scuola interregionale di Polizia locale
Regioni Emilia-Romagna/Liguria/Toscana

LA VIDEOSORVEGLIANZA

Gli aspetti generali e le specificità nell'ambito della sicurezza urbana e delle competenze comunali

Avv. Andrea Reghelin

Modena, 27/11/2015

Scuola Interregionale di Polizia Locale

Indice del documento

- Poteri del Sindaco e competenze in materia di sicurezza
- Codice in materia di protezione dei dati personali: aspetti generali
- Videosorveglianza ed Enti Locali
- La videosorveglianza all’interno dei luoghi di lavoro
- Il nuovo Regolamento europeo
- Videosorveglianza e Cloud

Poteri del Sindaco e competenze in materia di sicurezza

Normativa di riferimento

- Regio decreto 18 giugno 1931, n. 773 «*Approvazione del testo unico delle leggi di pubblica sicurezza*» (c.d. T.U.L.P.S.).
- D. Lgs. 18 agosto 2000, n. 267 «*Testo unico delle leggi sull'ordinamento degli Enti Locali*» (c.d. T.U.E.L.).
- Legge 26 marzo 2001 n. 128 «*Interventi legislativi in materia di tutela della sicurezza dei cittadini*» Decreto Ministero Interno 07/04/2008 n° 104 - Regolamento previsto dall'articolo 17, comma 3, della legge 26 marzo 2001, n. 128, recante «Interventi legislativi in materia di tutela della sicurezza dei cittadini».
- Decreto legge 23 maggio 2008, n. 92 recante «*Misure urgenti in materia di sicurezza pubblica*» convertito con Legge 24 luglio 2008, n. 125 «*Conversione in legge, con modificazioni, del decreto-legge 23 maggio 2008, n. 92, recante misure urgenti in materia di sicurezza pubblica*».

Poteri del Sindaco

- Ai sensi dell'art. 50 del Testo Unico Enti Locali (TUEL) il Sindaco:
  - è l'organo «**responsabile dell'amministrazione del Comune**»
  - svolge ulteriori «**funzioni attribuitegli quale autorità locale nelle materie previste da specifiche disposizioni di legge**».
- In particolare, per far fronte ai sempre più frequenti fenomeni di micro-criminalità e per garantire maggior tutela della sicurezza urbana, il legislatore ha affidato al Sindaco molteplici funzioni connesse alla **sicurezza ed incolumità pubblica**.

Poteri del Sindaco

- Il processo di conferimento al Sindaco di questi compiti è culminato nel **Decreto legge 23 maggio 2008, n. 92 recante «misure urgenti in materia di sicurezza pubblica»** (convertito, con modificazioni, con legge 24 luglio 2008, n. 125), parte integrante di una serie articolata di misure legislative in materia di sicurezza approvate dal Consiglio dei Ministri del 21 maggio 2008 (il c.d. *pacchetto sicurezza*).

- Tale decreto, infatti, ha riconosciuto **ulteriori poteri ai Sindaci in materia di controllo del territorio** e **contrasto del degrado urbano**: l'**art. 6** della suddetta normativa, in particolare, ha modificato l'art. 54 TUEL, rubricato «***Attribuzioni del sindaco nelle funzioni di competenza statale***», ampliando le attribuzioni del Sindaco fino ad affidargli il ruolo di "**garante della sicurezza urbana**".

Attribuzioni del Sindaco nelle funzioni di competenza statale

Ai sensi dell'**art. 54 T.U.E.L.** quindi, il Sindaco, quale ufficiale del Governo, sovrintende:

- all'**emanazione degli atti che gli sono attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica** (funzione di indirizzo e di programmazione generale)

- allo **svolgimento delle funzioni affidategli dalla legge in materia di pubblica sicurezza e di polizia giudiziaria**;

- alla **vigilanza su tutto quanto possa interessare la sicurezza e l'ordine pubblico, informandone il prefetto**.

I provvedimenti del Sindaco: le ordinanze

- I Sindaci sono autorizzati ad intervenire attraverso l'emanazione di atti (cd. **ordinanze**) per **prevenire e contrastare fenomeni** (puniti anche sul versante penale), quali:
  - attività criminose, come lo spaccio di stupefacenti, lo sfruttamento della prostituzione, l'accattonaggio con impiego di minori e disabili e i fenomeni di violenza legati anche all'abuso di alcool;
  - danneggiamento al patrimonio pubblico e privato e fenomeni di scadimento della qualità urbana;
  - intralcio alla pubblica viabilità, alterazione del decoro urbano, abusivismo commerciale e illecita occupazione di suolo pubblico;
  - prostituzione su strada e comportamenti contro la pubblica decenza.

Provvedimenti del Sindaco: le ordinanze comunali

- In generale, le ordinanze comunali sono **provvedimenti emanati per imporre o per vietare un determinato comportamento** ad un singolo soggetto, ad una specifica categoria di persone, ovvero a tutti indistintamente i consociati.
- Si tratta quindi di atti che creano:
  - **obblighi o doveri positivi** (*facere*)
  - **divieti o doveri negativi** (*non facere*)

  la cui inosservanza comporta l'applicazione di una **sanzione** a carico dell'inadempiente.
- Nell'ambito dell'ordinamento comunale possono essere emanate:
  - **ordinanze ordinarie**
  - **ordinanze contingibili ed urgenti**.

Provvedimenti del Sindaco: le ordinanze comunali

- Le **ordinanze ordinarie** sono provvedimenti adottati sul fondamento ed in applicazione di **disposizioni di legge o di regolamento**, sia dal Sindaco, sia dai funzionari comunali competenti (dirigenti o responsabili di servizio).

- Le **ordinanze contingibili ed urgenti** sono provvedimenti **di esclusiva competenza del Sindaco**, o di chi lo sostituisce, che possono essere emanati **anche in deroga alle vigenti norme di legge e di regolamento** (ma non ai suoi principi generali, né a norme costituzionali).

Le ordinanze contingibili ed urgenti

- Quale ufficiale del Governo, il Sindaco può adottare **provvedimenti contingibili e urgenti al fine di prevenire e di eliminare gravi pericoli che minacciano l'incolumità pubblica e la sicurezza urbana**.
- La legge di riforma non ha tuttavia dato alcuna **definizione di «incolumità pubblica» e di «sicurezza urbana»**, facendo così sorgere molteplici dubbi interpretativi relativamente ai contenuti di tali presupposti di emanazione delle ordinanze contingibili ed urgenti.
- La **Corte Costituzionale**, con sentenza n. 196/2009, a seguito di un ricorso per denunciato contrasto con l'autonomia costituzionalmente garantita di enti territoriali, è intervenuta dichiarando che è compito dello Stato:
  - definire le nozioni di "incolumità pubblica" e di "sicurezza urbana" previste dalla legge
  - individuare le situazioni in cui i sindaci sono autorizzati ad adottare provvedimenti di pubblica sicurezza e di ordine pubblico

Incolumità pubblica e Sicurezza urbana

- Successivamente, il **Ministro dell'Interno**, con **decreto del 5 agosto 2008**, ha precisato che:
  - l'**incolumità pubblica** riguarda l'integrità fisica della popolazione
  - la **sicurezza urbana** è "**un bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale**".

Presupposti delle ordinanze contingibili ed urgenti

- I presupposti che giustificano l'emanazione, da parte del Sindaco, delle ordinanze sono:
  - il verificarsi di un **evento abnorme, accidentale, eccezionale, inaspettato**;
  - l'**impossibilità di fare fronte, con gli strumenti ordinari, alla situazione di pericolo imminente ed attuale**.
- La legge impone al Sindaco di fornire, a supporto delle ordinanze, **motivazioni:**
  - **adeguate,**
  - **logiche,**
  - **stringenti**
  - **approfondite.**

Presupposti delle ordinanze contingibili ed urgenti

- Per la legittimità dei provvedimenti, inoltre, è necessario che gli stessi siano:
  - **Logici**
  - **Proporzionati**

  posto che l'ordinanza deve rappresentare lo **strumento meno gravoso possibile a carico dei soggetti destinatari**.

- Le ordinanze contingibili ed urgenti devono avere una **durata limitata nel tempo**, in relazione alle c.d. "**esigenze obiettive**" della fattispecie concreta.

Presupposti delle ordinanza contingibili ed urgenti

- I suddetti provvedimenti ordinativi, ai sensi del novellato art. 54 T.U.E.L., devono essere **preventivamente e tempestivamente comunicati al Prefetto anche ai fini della predisposizione degli strumenti ritenuti necessari alla loro attuazione**.

  – Al **Prefetto** spetta, oltre che il **potere di ispezione**, il compito di **disporre delle misure necessarie per il concorso delle forze di polizia per assicurare l'attuazione delle ordinanze sindacali**.

Giurisprudenza

- «La potestà del Sindaco di adottare, quale Ufficiale del Governo, **provvedimenti contingibili e urgenti** ex art. 54 comma 2, D.Lgs. n. 267 del 2000, **è strettamente finalizzata a prevenire ed eliminare gravi pericoli che minacciano l'incolumità dei cittadini**. Il potere di urgenza può essere esercitato solo per affrontare **situazioni di carattere eccezionale ed impreviste**, costituenti **concreta minaccia per la pubblica incolumità**, per le quali sia **impossibile utilizzare i normali mezzi apprestati dall'ordinamento giuridico** e unicamente in presenza di un preventivo accertamento della situazione che deve fondarsi su prove concrete e non su mere presunzioni. Gli anzidetti presupposti non ricorrono se il Sindaco può fronteggiare la situazione con rimedi di carattere corrente nell'esercizio ordinario dei suoi poteri o la situazione può essere prevenuta con i normali strumenti apprestati dall'ordinamento.» (Consiglio Stato , sez. V, 11 dicembre 2007 , n. 6366)

Giurisprudenza

- Secondo la consolidata giurisprudenza i presupposti per l'adozione dei provvedimenti contingibili ed urgenti sono:
  - da un lato, l'impossibilità di differire l'intervento ad altra data in relazione alla ragionevole previsione di danno incombente (**carattere d'urgenza**)
  - dall'altro l'impossibilità di provvedere con gli ordinari mezzi offerti dalla legislazione (**contingibilità**).
- Il requisito della contingibilità è soddisfatto quando **il pericolo non è evitabile con gli ordinari mezzi dell'amministrazione**; in altri termini, **la situazione imprevedibile di grave pericolo per la sicurezza urbana, in ordine alla quale il Sindaco ritiene di intervenire immediatamente con questo tipo di ordinanza, non deve trovare disciplina in altra norma statale, regionale o comunale** (Cons. Stato, sez. 2°, n. 1904 del 2.4.2001).

Ulteriori poteri del Sindaco

- Il Sindaco **concorre ad assicurare anche la cooperazione della polizia locale con le Forze di polizia statali**, nell'ambito delle direttive di coordinamento impartite dal Ministro dell'interno - Autorità Nazionale di Pubblica Sicurezza.
  - La **Polizia Locale** considerata dall'art. 54 T.U.E.L. sembra essere la sola **Polizia Municipale**, posto che le Polizie Provinciali, pur appartenendo alla più ampia categoria della Polizia Locale, non dipendono dal Sindaco.
  - La definizione delle **modalità per la cooperazione** tra Polizia Locale e forze di Polizia Statali è demandata all'adozione di **apposite direttive da parte del Ministro dell'Interno**: i provvedimenti finalizzati a prevenire ed eliminare gravi pericoli che minacciano l'incolumità pubblica e la sicurezza urbana devono pertanto essere adottati nel rispetto di tali eventuali atti di indirizzo ministeriali.
- Il Sindaco, inoltre, ha la facoltà di **impartire direttive per l'esercizio delle funzioni connesse alla Polizia Locale** (art. 2 della Legge 7 marzo 1986, n. 65 (Legge-quadro sull'ordinamento della polizia municipale).

Ulteriori poteri del Sindaco

- Un ulteriore potere affidato ai Sindaci al fine di tutelare la sicurezza urbana è contenuto nel comma 6 dell'art. 54 T.U.E.L. ove si legge:: «*quando a causa di circostanze straordinarie si verifichino particolari necessità dell'utenza o per motivi di sicurezza urbana,* ***il sindaco può modificare gli orari degli esercizi commerciali, dei pubblici esercizi e dei servizi pubblici, nonché, d'intesa con i responsabili territorialmente competenti delle amministrazioni interessate, gli orari di apertura al pubblico degli uffici pubblici localizzati nel territorio***».

Codice in materia di protezione dei dati personali: aspetti generali

Definizioni, principi generali, adempimenti

Dato personale/Dato anonimo

Dato Personale:

•Qualunque informazione relativa ad una persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

•Per esempio informazioni relative ad un lavoratore (nome, cognome, data e luogo di nascita, stipendio, ecc …).

•I dati relativi a **persone giuridiche, imprese, enti o associazioni non sono dati personali e pertanto non sono più soggetti all'applicazione del Codice per la protezione dei dati personali** (articolo 4, comma 1, lett. del D.lgs. 196/2003 modificato dal D.L. 205/2011).

Dato anonimo:

•Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Dato sensibile/Dato giudiziario

- **Dato sensibile è un dato personale idoneo a rivelare:**
  - L'origine razziale ed etnica
  - Le convinzioni religiose, filosofiche o di altro genere (es: permessi per festività religiose)
  - Le opinioni politiche
  - L'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale (es: trattenuta sindacale)
  - Lo stato di salute e la vita sessuale (es: certificato di malattia)
- **Dato giudiziario è un dato personale idoneo a rivelare:**
  - I provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti
  - la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale

Trattamento

- Per trattamento dei dati personali si intende **qualunque operazione o complesso di operazioni concernenti i dati**, anche se non registrati in una banca di dati in particolare:

la raccolta **la registrazione** **l'organizzazione** **la conservazione** **la consultazione** **l'elaborazione** **la modificazione** **la selezione** **l'estrazione**	**Il raffronto** **l'utilizzo** **l'interconnessione** **il blocco** **la comunicazione** **la diffusione** **la cancellazione** **la distruzione**

Trattamento effettuati per finalità amministrativo-contabili

- Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo **svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile**, **a prescindere dalla natura dei dati trattati.**

  In particolare, perseguono tali finalità:

  – le attività organizzative interne,
  – le attività funzionali all'adempimento di obblighi contrattuali e precontrattuali,
  – le attività funzionali alla gestione del rapporto di lavoro in tutte le sue fasi,
  – le attività funzionali alla tenuta della contabilità
  – le attività funzionali all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

  (articolo 34, comma 1-ter del D.lgs 196/2003 introdotto dal D.L. 70/2011)

Trattamento che presenta dei rischi specifici

- **Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato**, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, **è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato**, prescritti dal Garante in applicazione dei principi sanciti dal codice, nell'ambito di una **verifica preliminare all'inizio del trattamento**, effettuata anche in relazione a **determinate categorie di titolari o di trattamenti**, anche a seguito di un interpello del titolare.

- Il Garante ha adottato diversi provvedimento nei confronti di categorie di titolari o di trattamenti che riguardano rischi specifici, tra essi, a titolo esemplificativo, il *Provvedimento generale prescrittivo in tema di biometria* (Deliberazione n. 513 del 12 novembre 2014)

Titolare del trattamento

- **Titolare del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
  - Es: La Società è il Titolare del trattamento

- Quando il trattamento è effettuato da una **persona giuridica**, da una **pubblica amministrazione** o da un qualsiasi altro **ente**, **associazione od organismo**, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Ambito di applicazione del Codice

- Il Codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da **chiunque è stabilito nel territorio dello Stato** o **in un luogo comunque soggetto alla sovranità dello Stato**.
- Il Codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di **un Paese non appartenente all'Unione europea** e impiega, per il trattamento, **strumenti situati nel territorio dello Stato** anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea.
- In caso di applicazione del Codice, **il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali**.

Responsabile del trattamento

- **Responsabile del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposti dal titolare al trattamento di dati personali**.
  - Es: società che forniscono servizi informatici
- Il responsabile è designato dal titolare **facoltativamente**.
- Se designato, il responsabile è individuato **tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento**, ivi compreso il profilo relativo alla sicurezza.
- Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

Responsabile del trattamento

- I compiti affidati al responsabile sono analiticamente specificati **per iscritto** dal titolare.
- Il responsabile effettua il trattamento attenendosi alle **istruzioni impartite dal titolare** il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, e delle proprie istruzioni.

Incaricati del trattamento

- **Incaricati** sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.
  - Es: i dipendenti di una società
- Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
- La designazione è effettuata **per iscritto** e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Interessato

- **Interessato**
  - La **persona fisica cui si riferiscono i dati personali** (Es: il cliente persona fisica)
  - Le **persone giuridiche, imprese, enti o associazioni non sono più interessati** ai sensi del Codice per la protezione dei dati personali (articolo 4, comma 1, lett. del D.lgs 196/2003 modificato dal D.L. 205/2011).

Contraente/Utente

- **Contraente**

  Qualunque **persona fisica, persona giuridica, ente o associazione** parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate.

- **Utente**

  Qualsiasi **persona fisica** che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

Comunicazione/Diffusione

- **Comunicazione**
  - Il dare conoscenza dei dati personali a uno o più soggetti determinati **diversi dall'interessato, dal responsabile e dagli incaricati**, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
  - Es: comunicazione di dati relativi ai dipendenti all'INPS

- **Diffusione**
  - Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
  - Es: bacheca accessibile al pubblico

Principi generali

- I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità (c.d. **principio di necessità**).
- I dati personali oggetto di trattamento sono:
  - trattati in modo lecito e secondo correttezza (c.d. **principio di liceità**);
  - raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi (c.d. **principio di finalità**);
  - esatti e, se necessario, aggiornati;
  - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati (c.d. **principio di proporzionalità**);
  - conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
- I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Informativa

- Ogni volta che vengono raccolti i dati personali di un interessato, ad esso verrà resa un’**informativa** che riporti tutti i dettagli relativi al trattamento ed in particolare:
  a. le finalità e le modalità del trattamento cui sono destinati i dati;
  b. la natura obbligatoria o facoltativa del conferimento dei dati;
  c. le conseguenze di un eventuale rifiuto di rispondere;
  d. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
  e. i diritti dell’interessato;
  f. gli estremi identificativi del titolare e, se designato del responsabile del trattamento.

Informativa

- L'informativa contiene anche gli elementi previsti da specifiche disposizioni del Codice e può non comprendere gli elementi già noti alla persona che fornisce i dati.
- Il Garante può individuare con proprio provvedimento **modalità semplificate** per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

Informativa

- Se i dati personali **non sono raccolti presso l'interessato**, l'informativa, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione, tranne quando:
  - i dati sono trattati in base ad un **obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria**;
  - i dati sono trattati ai fini dello svolgimento delle **investigazioni difensive** di cui alla legge n. 397/2000, o, comunque, per **far valere o difendere un diritto in sede giudiziaria**, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
  - l'informativa all'interessato comporta un **impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato**, ovvero si riveli, a giudizio del Garante, impossibile.

Consenso

- Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.
- Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.
- Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici**, i soggetti pubblici non devono richiedere il consenso dell'interessato.**

Notificazione

- Il Titolare del trattamento deve notificare preventivamente al Garante il trattamento di dati personali cui intende procedere, quando il trattamento riguarda, oltre ad altri casi,
  - dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
  - dati personali trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo;
  - dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Notificazione

- La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.
- La notificazione è validamente effettuata solo se è trasmessa attraverso il sito del Garante, utilizzando l'apposito modello e sottoscritta con firma digitale.
- Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.

Divieti di comunicazione e diffusione

La **comunicazione e la diffusione** sono **vietate**, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:

•in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;

•per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.

Cessazione del trattamento

In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

- distrutti;
- ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
- conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta.

Le misure di sicurezza

Misure idonee di sicurezza

- I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione:
  - alle conoscenze acquisite in base al progresso tecnico
  - alla natura dei dati
  - alle specifiche caratteristiche del trattamento

  in modo da ridurre al minimo, mediante l'adozione di **idonee e preventive** misure di sicurezza i rischi di:
  - distruzione o perdita, anche accidentale, dei dati stessi
  - accesso non autorizzato
  - trattamento non consentito o non conforme alle finalità della raccolta.

Misure minime di sicurezza

- I titolari del trattamento sono comunque tenuti ad adottare le misure minime previste dall'allegato B al d.lgs 196/2003 per i:
  - **Trattamenti effettuati con l'ausilio di strumenti elettronici**
    - autenticazione informatica;
    - adozione di procedure di gestione delle credenziali di autenticazione;
    - utilizzazione di un sistema di autorizzazione;
    - aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
    - protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
    - adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

Misure minime di sicurezza

- I titolari del trattamento sono comunque tenuti ad adottare le misure minime previste dall'allegato B al d.lgs 196/2003 per i:
  - **Trattamenti effettuati senza l'ausilio di strumenti elettronici**
    - aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
    - previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
    - previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il documento programmatico sulla sicurezza

- L’obbligo di elaborazione del DPS è stato abrogato dal Decreto Legge n. 5/2012 (c.d. decreto semplificazioni).

- Il documento programmatico sulla sicurezza più essere elaborato facoltativamente dal titolare del trattamento quale misura idonea di sicurezza.

Misure minime di sicurezza

MISURE MINIME DI SICUREZZA - ALLEGATO B AL D.LGS 196/2003		
TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI		
	TIPOLOGIA DI DATI A CUI APPLICARE LA MISURA	**SPECIFICHE**
Individuazione degli Incaricati	Tutti	Per iscritto
Sistema di autenticazione informatica	Tutti	Applicare punti da 1 a 11 dell'allegato B al D.lgs 196/03
Attribuzione User-Id e Password a ciascun incaricato	Tutti	Applicare il punto 2 dell'allegato B al D.lgs 196/03
Unicità User-Id	Tutti	Individuale e non riutilizzato
Password	Tutti	Segreta Min 8 caratteri Non contiene riferimenti riconducibili all'incaricato
Sostituzione Password	Tutti	Autonoma Al primo utilizzo Dati comuni ogni sei mesi Dati sensibili o giudiziari ogni tre mesi
Istruzioni in merito alla custodia del personal computer	Tutti	Per iscritto

Gli strumenti di tutela

Diritti dell'interessato
(articolo 7 d.lgs 196/2003)

1. L'interessato ha diritto di **ottenere la conferma dell'esistenza** o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di **ottenere l'indicazione**:
   a. dell'**origine** dei dati personali;
   b. delle **finalità e modalità** del trattamento;
   c. della **logica** applicata in caso di trattamento effettuato con **l'ausilio di strumenti elettronici**;
   d. degli estremi **identificativi** del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2 del Codice.
   e. dei soggetti o delle categorie di soggetti ai quali i dati personali **possono essere comunicati o che possono venirne a conoscenza** in qualità di rappresentante designato nel territorio dello Stato, di **responsabili o incaricati**.

Diritti dell'interessato
(articolo 7 d.lgs 196/2003)

3. L'interessato ha diritto di **ottenere**:
    a. l'**aggiornamento**, la **rettificazione** ovvero, quando vi ha interesse, l'**integrazione** dei dati;
    b. la **cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge**, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
    c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, **di coloro ai quali i dati sono stati comunicati o diffusi**, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

Diritti dell'interessato
(articolo 7 d.lgs 196/2003)

4. L'interessato ha diritto di **opporsi, in tutto o in parte**:
    a. per **motivi legittimi** al trattamento dei dati personali che lo riguardano, **ancorché pertinenti allo scopo della raccolta**;
    b. al trattamento di dati personali che lo riguardano **a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.**

Diritti dell’interessato

- I diritti sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato.
- La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
- Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
- Il riscontro alla richiesta da parte del titolare o del responsabile è fornito entro 15 giorni dal suo ricevimento.

Diritti dell’interessato

- Entro il termine di 15 giorni. Se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di 30 giorni dal ricevimento della richiesta medesima.
- I diritti non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso, se i trattamenti di dati personali sono effettuati in particolare :
  - ai fini dello svolgimento delle investigazioni difensive di cui alla legge n. 397/2000 o per far valere o difendere un diritto in sede giudiziaria, limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria.

Diritti dell’interessato

- L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la **rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo**, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Tutela dinanzi al Garante

L'interessato può rivolgersi al Garante:

- mediante reclamo circostanziato, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
- mediante segnalazione, se non è possibile presentare un reclamo circostanziato al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
- mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 d.lgs 196/2003

Tutela giurisdizionale

- Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione sono attribuite all'autorità giudiziaria ordinaria.

Le sanzioni

Sanzioni amministrative

SANZIONI AMMINISTRATIVE	
Art 161 **Omessa o inidonea informativa all'interessato**	6.000 € - 36.000 €
Art. 162, comma 2-bis **Mancata applicazione di norme in materia di:** - Misure minime di sicurezza - Consenso al trattamento - Trattamenti che presentano rischi specifici - Dati sensibili - Dati giudiziari - Divieti di comunicazione e di diffusione - Trasferimenti vietati al di fuori della UE - Comunicazioni indesiderate	10.000 € - 120.000 €
Art. 162, comma 2-ter **Inosservanza dei provvedimenti del Garante** - Provvedimenti di prescrizione di misure necessarie - Provvedimenti di divieto	30.000 € - 180.000 €
Art. 163 **Omessa o incompleta notificazione**	20.000 € - 120.000 €
Art. 164 **Omessa informazione o esibizione al Garante**	10.000 € - 60.000 €
Art. 165 **Sanzione accessoria**	pubblicazione dell'ordinanza-ingiunzione

Sanzioni penali

SANZIONI PENALI	
Art. 167 Trattamento illecito di dati	
Consenso	Reclusione da sei mesi a diciotto mesi
Comunicazione e diffusione	Reclusione da sei a ventiquattro mesi
Trattamenti che presentano rischi specifici Dati sensibili Dati giudiziari Divieti di comunicazione e di diffusione Trasferimenti vietati al di fuori della UE Comunicazioni indesiderate	Reclusione da uno a tre anni
Art. 168 **Falsità nelle dichiarazioni e notificazioni al Garante**	Reclusione da sei mesi a tre anni
Art. 169 **Omessa adozione delle misure di sicurezza**	Arresto fino a 2 anni
Prescrizione di un termine per la regolarizzazione Adempimento nei 60 g che seguono il termine	¼ del massimo della sanzione amministrativa Estinzione del reato
Art. 170 **Inosservanza di provvedimenti del Garante** Autorizzazioni Provvedimento adottati in caso di ricorso Provvedimento adottati in caso di reclamo	Reclusione da sei mesi a due anni
Art. 172 **Sanzione accessoria**	Pubblicazione della sentenza

Responsabilità civile

- Il legislatore equipara il trattamento dei dati personale ad una ***attività pericolosa***. Si tratta pertanto di una responsabilità per attività pericolose (art. 2050 c.c.)

- Vige in questo caso un principio del **ribaltamento dell'onere della prova**: spetta al danneggiante provare di avere adottato tutte le misure idonee ad evitare il danno.

- Il danneggiante è tenuto al risarcimento del **danno patrimoniale** e del **danno non patrimoniale.**

Codice Privacy e Videosorveglianza

- La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini mediante sistemi di videosorveglianza, configurano un **trattamento di dati personali**.
- L'art. 134 del Codice della Privacy, nel prevedere che il Garante promuova la sottoscrizione di un codice deontologico e buona condotta, definisce la videosorveglianza "***il trattamento effettuato con strumenti elettronici di rilevamento immagini***".
- Tale definizione va integrata con quelle contenute nei numerosi casi sottoposti all'esame dell'Autorità Garante della Privacy attraverso reclami, segnalazioni e richieste di parere, in cui si fa riferimento ad "***apparecchiature audiovisive che rilevano in modo continuativo immagini, eventualmente associate a suoni, relative a persone identificabili, spesso anche con registrazione e conservazione di dati***."
  - La regolamentazione dell'utilizzo di sistemi di videosorveglianza è prevalentemente opera del Garante, il quale, attraverso numerosi provvedimenti e pareri, ha fornito il quadro normativo di riferimento.

Codice Privacy e Videosorveglianza

- Il Codice (art. 18-22) consente ad un **soggetto pubblico** di effettuare attività di videosorveglianza solo ed esclusivamente per **svolgere funzioni istituzionali** (che deve individuare ed esplicitare con esattezza) di cui sia realmente titolare.
- Per un soggetto pubblico, quindi, non è lecito procedere all'installazione di sistemi di videosorveglianza in intere aree cittadine, senza **adeguate esigenze**.
  - Ad esempio, risulta priva di giustificazione l'installazione di impianti di videosorveglianza al solo fine di controllare il rispetto del divieto di fumare, di gettare mozziconi o di calpestare aiuole.

Videosorveglianza ed Enti Locali

Videosorveglianza e Sicurezza Urbana

- Ai sensi dell'articolo 1 del T.U.L.P.S. "*l'autorità di pubblica sicurezza* ***vigila al mantenimento dell'ordine pubblico, alla sicurezza dei cittadini, alla loro incolumità e alla tutela della proprietà****; cura l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle Province e dei Comuni, nonché delle ordinanze delle autorità*".
- Da circa un decennio **la videosorveglianza costituisce lo strumento privilegiato dai Comuni per intervenire sulla sicurezza del territorio.**
- Come si legge nella **Circolare Ministero dell'Interno 8 febbraio 2005** "*Sistemi di videosorveglianza. Definizione di linee guida in materia*», si tratta di **sistemi che effettuano «*una vera e propria attività di vigilanza su persone e beni, sostituendo, in tutto o in parte, la presenza umana sul posto***».

Videosorveglianza e Sicurezza Urbana

- Gli impianti di videosorveglianza installati dagli Enti Locali comunali sono generalmente finalizzati:
  - a **prevenire e reprimere** gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana", così come individuata secondo il Decreto Ministro Interno 5 agosto 2008;
  - a **tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale** e a prevenire eventuali atti di vandalismo o danneggiamento;
  - al **controllo** di determinate aree;
  - al **monitoraggio** del traffico.

Videosorveglianza e Sicurezza Urbana

- Più dettagliatamente, il Sindaco può adottare sistemi di videosorveglianza per **prevenire e contrastare**:
  - le **situazioni urbane di degrado** che favoriscono l'insorgere di fenomeni criminosi, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, l'accattonaggio con impiego di minori e disabili e i fenomeni di violenza legati anche all'abuso di alcool;
  - il **danneggiamento del patrimonio pubblico e privato** con conseguenze non solo economiche, ma che determinano lo scadimento della qualità urbana;
  - fenomeni di **abusivismo commerciale** e di **illecita occupazione di suolo pubblico**;
  - schiamazzi o **comportamenti che possono turbare gravemente la quiete pubblica o il libero utilizzo degli spazi pubblici o la fruizione cui sono destinati**.

Sicurezza Urbana e Privacy

- I dispositivi di videosorveglianza adottati dagli Enti Locali per fini istituzionali devono, in ogni caso, coniugare il valore della sicurezza urbana con quello della privacy: attraverso le telecamere, infatti, gli organi pubblici, devono tutelare la riservatezza della cittadinanza.
- Il ricorso a strumenti di videosorveglianza da parte di Enti Locali, pertanto, è possibile purché non determini un'**ingerenza ingiustificata** nei diritti e nelle libertà fondamentali degli individui.

Interferenze illecite nella vita privata

- L'**art. 615 bis c.p**. disciplina l'ipotesi delittuosa rubricata «**interferenze illecite nella vita privata**».
- La norma punisce **chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata** svolte nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi.
- Il concetto di "**privata dimora**" è stato interpretato dalla Cassazione in senso estensivo, ricomprendendo **tutti quegli ambiti in cui si svolge (anche occasionalmente) la vita privata degli individui e su cui gli stessi abbiano tendenzialmente lo *jus escludendi* di terzi**. (Cass., Sez.V, 5/10/2004, n. 16189).
- Sotto il profilo soggettivo, il reato di interferenze illecite nella vita privata richiede il **dolo generico**, che consiste nella **volontà cosciente** dell'agente di procurarsi indebitamente immagini inerenti la "privacy" altrui.

  - Applicando questo principio, la Cassazione, per esempio ha ritenuto **sussistente tale reato nel caso di installazione di una videocamera collocata in modo da riprendere la soglia di casa e l'ingresso della autorimessa della parte offesa** (Cass. pen., Sez. I, 4/4/2003, n. 25666).

Interferenze illecite nella vita privata

- La Cassazione ha chiarito con l'art. 615-bis c.p. *"il legislatore avrebbe inteso sanzionare le* ***incursioni abusive (ancorché non fisiche) nella vita privata altrui, fissate con strumenti tecnici suscettibili di riprodurre la violazione di ambiti riservati e preclusi all'osservazione indiscreta dei terzi****. La lesione della riservatezza può pertanto consumarsi, attraverso illecite interferenze anche nei locali ove si svolge il lavoro dei privati (studio professionale, ristorante, bar, osteria, negozio in genere).* ***La facoltà di accesso da parte del pubblico*** – ha evidenziato la Cassazione – ***non fa venire meno nel titolare il diritto di escludere singoli individui non autorizzati ad entrare o a rimanere****"* (Cass. pen., Sez. V, 5/12/2005, n. 10444).

Sicurezza Urbana e Privacy

- **<u>Principali diritti e libertà degli individui</u>:**

  – **libertà di movimento** intesa non solo come diritto di andare in un luogo - che non viene quasi mai fisicamente vietato a nessuno - ma piuttosto come diritto di muoversi senza lasciare necessariamente traccia di dove si è stati.

  – **libertà di espressione e di associazione**: dispositivi di videosorveglianza in grado di registrare suoni e immagini possono sia scoraggiare comportamenti legittimi di dissenso quali manifestazioni e proteste, che generare fraintendimenti sulle opinioni espresse dalla persona che è stata filmata.

  – **diritto a non essere discriminati**: la visione attraverso la telecamera di persone trasandate o di una precisa origine etnica, ad esempio, ha portato al loro allontanamento da alcuni centri commerciali senza che queste persone si fossero rese responsabili di comportamenti dannosi o di tentativi di furto, scopi per cui le telecamere erano peraltro state installate.

Normativa di riferimento

- Come già anticipato, la materia è disciplinata **dalle disposizioni generali in tema di protezione dei dati personali**; più dettagliatamente:
  - dalle **disposizioni generali europee e nazionali previste in materia di protezione dei dati personali**;
  - dalle **disposizioni specifiche emanate dal Garante per la protezione dei dati personali**;
  - dalle altre **disposizioni dell'ordinamento applicabili**, quali ad esempio le vigenti norme dell'ordinamento civile e penale in materia di:
    - interferenze illecite nella vita privata sul controllo a distanza dei lavoratori
    - sicurezza presso stadi e impianti sportivi,
    - musei, biblioteche statali e archivi di Stato
    - impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali
    - porti, stazioni ferroviarie, stazioni delle ferrovie metropolitane e linee di trasporto urbano

Principale normativa europea

- **Proposta di Regolamento** del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), (COM(2012) 11) - 25 gennaio 2012.

- **Direttiva 95/46/CE** del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

Principale normativa italiana

- Decreto Legislativo 30 giugno 2003, n. 193 "**Codice in materia di protezione dei dati personali**»
- Decreto legge 23 maggio 2008, n.92 recante «**Misure urgenti in materia di sicurezza pubblica**» (convertito nella Legge 24 luglio 2008, n. 125) decreto-legge 23 febbraio 2009, n. 11, recante "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori" (convertito nella Legge 23 aprile 2009, n. 38)
- **Circolare Ministero dell'Interno 8 febbraio 2005** Prot. n. 558/A/421.2/70/456 "**Sistemi di videosorveglianza. Definizione di linee guida in materia**"
- **Circolare Ministero dell'Interno 6 agosto 2010** Prot. n. 558/A/421.2/70/195960 "**Sistemi di videosorveglianza**"
- **Direttiva Ministero dell'Interno** Prot n. 558/SICPART/421.2/70 "**Sistemi di videosorveglianza in ambito comunale**"

I Provvedimenti del Garante

Scuola Interregionale di Polizia
Locale

Provvedimenti dell'Autorità Garante per la protezione dei dati personali

- **Provvedimenti generali**
  - *Il decalogo delle regole per non violare la privacy* del 29 novembre 2000
  - *Provvedimento generale sulla videosorveglianza del 29 aprile 2004*
  - *Provvedimento generale sulla videosorveglianza* dell'8 aprile 2010

- **Altri provvedimenti**
  - Installazione da parte del comune di Milano di alcune telecamere in luogo pubblico del 17 dicembre 1997.
  - Installazione di alcune telecamere da parte di un comune del 28 maggio 1998.
  - Città di Torino - Videosorveglianza sui mezzi di trasporto pubblico urbano 23 marzo 1999.
  - Città di Portici - Impianto di telecontrollo e videosorveglianza 17 febbraio 2000.
  - Diritto di accesso - Accesso ai dati acquisiti mediante un impianto di videosorveglianza - 19 dicembre 2001.

Provvedimenti dell'Autorità Garante per la protezione dei dati personali

- In materia di videosorveglianza, il Garante si è pronunciato in più occasioni adottando alcuni provvedimenti con i quali è richiamata l'attenzione sulla necessità che i sistemi di rilevazione vengano attivati in presenza di un quadro articolato di **garanzie**.
- Più dettagliatamente:
  - nel comunicato stampa del 5 marzo 2000 «***Videosorveglianza: i comuni devono adeguare alla privacy la ripresa delle immagini***» ha ammonito gli enti locali che intendono dotarsi di sistemi di videosorveglianza del territorio e del traffico cittadino o di telecontrollo ambientale di **rispettare i principi fondamentali previsti dalla legge sulla privacy**.
    - Tra le cautele suggerite dal Garante a tutela della privacy dei cittadini ripresi dai sistemi video rileva soprattutto quella di **limitare le possibilità di ingrandimento delle riprese e il livello di dettaglio sui tratti somatici delle persone inquadrate dalle telecamere**.

Provvedimenti dell'Autorità Garante per la protezione dei dati personali

– successivamente, nel novembre 2000, portata a termine la prima indagine sulla presenza di telecamere visibili in Italia, il Garante ha emanato il primo **provvedimento di carattere generale** intitolato «***Decalogo delle regole per non violare la privacy***», al fine di sottolineare ulteriormente l'importanza che l'installazione di dispositivi per le videoriprese tuteli la libertà delle persone erispetti le norme sulla privacy (in particolare gli adempimenti, le garanzie e le tutele del Codice sulla protezione dei dati personali).

Provvedimento generale del Garante sulla videosorveglianza - 29 novembre 2004

- Con un ulteriore **provvedimento di carattere generale (29 novembre 2004)** il Garante Privacy ha individuato per la videosorveglianza un **decalogo di norme** da rispettare:
  - Individuare le finalità di sorveglianza e la compatibilità della stessa con le norme di settore vigenti.
  - Rispettare i principi di correttezza e liceità del trattamento.
  - Effettuare, se dovuta, la notificazione al Garante.
  - Fornire agli interessati una chiara e completa informativa.
  - Non violare il divieto di controllo a distanza dei dipendenti sancito nello statuto dei lavoratori.
  - Registrare le sole immagini indispensabili per perseguire lo scopo dichiarato, evitando, per quanto possibile, immagini dettagliate o ingrandite.

Provvedimento generale del Garante sulla videosorveglianza - 29 novembre 2004

- Individuare il periodo massimo di conservazione delle immagini.
- Nominare i soggetti responsabili ed incaricati del trattamento.
- Non utilizzare per altri scopi i dati raccolti.
- Per le telecamere situate agli accessi dei centri storici, o delle zone a traffico limitato, rispettare le disposizioni contenute nel DPR 250/1999 (con tale decreto è stato emanato il regolamento per la disciplina dell'autorizzazione all'installazione e all'esercizio di impianti elettronici e telematici per la rilevazione ed il sanzionamento della circolazione non autorizzata nelle corsie riservate).

- Il Garante Privacy ha ritenuto di dover modificare il suddetto provvedimento generale del 2004 a seguito dell'approvazione governativa dei decreti sicurezza del 2008-2009 i quali, come già anticipato, hanno conferito agli Enti Locali poteri in materia di controllo del territorio (anche tramite videosorveglianza) che in precedenza non esistevano.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Il provvedimento del 2010, rispetto a quello precedente, sostanzialmente ha previsto:
  - Una **diversa disciplina della videosorveglianza nel settore pubblico** e principalmente per quanto riguarda la videosorveglianza di intere zone del territorio comunale che in precedenza erano a vario titolo vietate.
  - In particolare il garante ammette in questo provvedimento, diversamente dal passato, la **creazione di sistemi integrati pubblici di videosorveglianza ad opera degli enti locali ammettendo implicitamente che il territorio comunale venga "coperto" di telecamere che potranno essere anche gestite dall'ente locale direttamente o per il tramite di soggetti esterni agli enti**.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Adozione di particolare cautele che si riassumono essenzialmente nella **tracciabilità:**
  - degli **accessi del personale**,
  - del requisito dell'**identificazione** specifica di chi ha accesso ai sistemi,
  - dell'**impossibilità di ricostruire percorsi dei singoli cittadini all'interno del territorio comunale**.
- Obbligo di mostrare l'informativa per il trattamento dei dati personali anche in modalità notturna.
- **Conservazione delle immagini da parte degli enti locali per sette giorni**, (diversamente dalla previgente disciplina che prevedeva il termine di poche ore o al massimo alle 24 ore successive), con la possibilità di conservare i dati per un termine ancor più lungo qualora vi siano esigenze di particolare conservazione che (in alcuni casi devono comunque essere sottoposti alle verifiche preliminari del Garante privacy).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Più dettagliatamente:

a. <u>Trattamento dei dati personali e videosorveglianza: principi generali</u>

– Il trattamento dei dati attraverso sistemi di videosorveglianza deve essere fondato su uno dei presupposti di **<u>liceità</u>** che il Codice prevede espressamente per i soggetti pubblici, ossia sullo **<u>svolgimento di funzioni istituzionali</u>** (*artt. 18-22 del Codice*).

– Un Ente Locale deve perseguire **<u>solo finalità di sua pertinenza</u>**, esclusivamente per scopi determinati, espliciti e legittimi.

- Ne consegue, ad esempio, l'impossibilità per un Sindaco di installare telecamere per la sorveglianza in una proprietà privata non sussistendo, in tal caso, alcuna finalità di sicurezza pubblica e di prevenzione dei reati (al pari, un privato cittadino può solo installare telecamere per la videosorveglianza della sua proprietà ma non per riprendere il suolo pubblico).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

– L'attività di videosorveglianza deve essere effettuata nel rispetto del c.d. **principio di proporzionalità** nella scelta delle modalità di ripresa e dislocazione nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (*art. 11, comma 1, lett. d) del Codice*).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

b. Adempimenti applicabili a soggetti pubblici e privati:

•L'INFORMATIVA

- Gli interessati **devono essere sempre informati che stanno per accedere in una zona videosorvegliata**; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

- A tal fine, il Garante ritiene che si possa utilizzare lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, già individuato ai sensi dell'art. 13, comma 3, del Codice.

- In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, **potranno essere installati più cartelli**.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Il supporto con l'informativa:
  - deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
  - deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
  - può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.
- In ogni caso il titolare, anche per il tramite di un incaricato, **ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata**, contenente gli elementi individuati dall'art. 13 del Codice.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

c. Informativa e videosorveglianza effettuata per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati

- L'obbligo di fornire una **preventiva informativa agli interessati**, **non è applicabile al trattamento di dati personali effettuato** (anche sotto forma di suoni e immagini) **da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati** (art. 53 del Codice) **nei casi in cui il trattamento stesso è effettuato in base ad espressa disposizione di legge che lo prevede specificamente**.
  - **Il Garante ritiene tuttavia fortemente auspicabile che l'informativa, benché non obbligatoria** sia comunque resa in tutti i casi nei quali **non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati**.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

– Deve invece essere **obbligatoriamente fornita un'idonea informativa** in tutti i casi in cui i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici **non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice** (es. utilizzo di sistemi di rilevazioni delle immagini per la contestazione delle violazioni del Codice della strada).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

d. Prescrizioni specifiche

•LA VERIFICA PRELIMINARE

- I trattamenti di dati personali nell'ambito di una attività di videosorveglianza **devono essere effettuati rispettando le misure e gli accorgimenti prescritti dall'Autorità Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare** (art. 17 del Codice), quando vi sono **rischi specifici** per i diritti e le libertà fondamentali e la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.
  - Ad esempio, devono essere sottoposti alla verifica preliminare i sistemi di videosorveglianza dotati di software che permetta il **riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate** (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima. Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Ulteriori casi in cui si rende necessario richiedere una verifica preliminare riguardano **l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione**, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso.
- Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel provvedimento del Garante non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, **il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità**.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- **ESCLUSIONE DELLA VERIFICA PRELIMINARE**
  - Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza **non deve richiedere una verifica preliminare** purché siano rispettate tutte le seguenti condizioni:

    a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;

    b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

    c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento adottato dal Garante.

.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- **NOTIFICAZIONE**
  - I trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (art. 37 del Codice).
  - Non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente.
  - La mancata o incompleta notificazione ai sensi degli artt. 37 e 38 del Codice è punita con la sanzione amministrativa prevista dall'art. 163.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

e. Misure di sicurezza da applicare ai dati personali trattati mediante sistemi di videosorveglianza e soggetti preposti

•MISURE DI SICUREZZA

- I dati raccolti mediante sistemi di videosorveglianza devono essere **protetti con idonee e preventive misure di sicurezza**, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).
- Devono quindi essere adottate specifiche **misure tecniche ed organizzative** che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- **Le misure minime di sicurezza devono rispettare i seguenti principi:**
  - in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati **diversi livelli di visibilità e trattamento delle immagini** (se tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di **credenziali di autenticazione** che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza);
  - laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente **limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione**;

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte **misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto.**

- nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare **specifiche cautele**; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

- qualora si utilizzino **apparati di ripresa digitali connessi a reti informatiche**, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale;

- la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa **applicazione di tecniche crittografiche che ne garantiscano la riservatezza**; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

f. Responsabili e incaricati

- **Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini** (deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni).
- Occorre altresì individuare **diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore**, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).
- Vanno infine osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento (art. 29 del Codice).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

g. Durata dell'eventuale conservazione

- Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere **commisurata al tempo necessario** - e predeterminato - a raggiungere la finalità perseguita.
- La conservazione deve essere **limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione**, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.
- Solo in alcuni casi, per peculiari **esigenze tecniche** o per la particolare **rischiosità dell'attività** svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un **tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana**.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- **Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione".**
- In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una **verifica preliminare del Garante**, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità.
- La congruità di un termine di tempo più ampio di conservazione va **adeguatamente motivata** con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale **cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto**, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
- Il mancato rispetto dei tempi di conservazione delle immagini raccolte e del correlato obbligo di cancellazione di dette immagini oltre il termine previsto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

h. Diritti degli interessati

- Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di **accedere ai dati che li riguardano**, di **verificare le finalità**, le **modalità** e la **logica del trattamento**.
  - La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.
- In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.
- Viceversa, l'interessato ha diritto di ottenere il **blocco dei dati** qualora essi siano trattati in violazione di legge.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

SETTORI SPECIFICI:

a. Sicurezza nel trasporto pubblico

- Alcune situazioni di particolare rischio possono fare ritenere lecita l'installazione di sistemi di videosorveglianza sia su **mezzi di trasporto pubblici**, sia presso le **fermate dei predetti mezzi**.
- La localizzazione delle telecamere e le modalità di ripresa, nel rispetto dei principi di necessità, proporzionalità e finalità devono **evitare riprese particolareggiate se non sono indispensabili in relazione alle finalità perseguite**.
- I titolari del trattamento devono provvedere a fornire la prevista **informativa agli utenti** del servizio di trasporto urbano.
- Specifiche cautele devono essere osservate **laddove vengano installati impianti di videosorveglianza presso le aree di fermata, in prossimità delle quali possono transitare anche soggetti diversi dagli utenti del servizio di trasporto pubblico.**

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- In particolare, l'angolo visuale delle apparecchiature di ripresa deve essere strettamente circoscritto all'area di permanenza, permettendo l'inquadratura solo della pensilina e di altri arredi urbani funzionali al servizio di trasporto pubblico (tabelle degli orari, paline recanti l'indicazione degli autobus in transito, ecc.), con esclusione della zona non immediatamente circostante e comunque dell'area non direttamente funzionale rispetto alle esigenze di sicurezza del sistema di traffico e trasporto.
- L'esistenza delle telecamere deve essere opportunamente evidenziata nelle aree di fermata.
- Il mancato rispetto di quanto prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

SETTORI SPECIFICI:

b. Sistemi integrati di videosorveglianza

- In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, si è incrementato il ricorso a **sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati**, nonché l'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, Internet service providers, fornitori di servizi video specialistici, ecc.).
- In tali circostanze, talvolta, le immagini riprese vengono rese disponibili, con varie tecnologie o modalità, alle forze di polizia.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Sono individuabili le seguenti **tipologie di sistemi integrati di videosorveglianza**:
  - gestione coordinata di funzioni e servizi tramite **condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento**, i quali utilizzano le medesime infrastrutture tecnologiche;
    - in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati.
  - **collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo**;
    - tale soggetto terzo, designato responsabile del trattamento da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- il Garante ritiene che in tali ipotesi si possa utilizzare il modello semplificato di informativa "minima" (indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia)
- Il collegamento telematico tra più titolari deve essere reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati.
- Sono richieste **specifiche misure di sicurezza** (ulteriori rispetto a quelle minime) quali:
  - L'adozione di sistemi idonei alla **registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate**, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;
  - La **separazione logica delle immagini registrate dai diversi titolari**.
    - In tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

c. Sicurezza urbana

- I Comuni che installano telecamere per fini di sicurezza urbana hanno l'obbligo di **mettere cartelli che ne segnalino la presenza**, salvo che le attività di videosorveglianza siano riconducibili a quelle di tutela specifica della sicurezza pubblica, prevenzione, accertamento o repressione dei reati.
- Per fini di sicurezza urbana la conservazione dei dati è ammessa fino a **7 giorni** che non possono essere superati, **fatte salve speciali esigenze**.
- In ogni caso il Garante ribadisce l'auspicio che, nelle predette ipotesi**, l'informativa, benché non obbligatoria, venga comunque resa,** specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- I Comuni e, in generale, i soggetti pubblici operanti sul territorio possono svolgere attività di **videosorveglianza in forma integrata,** tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.
  - I sistemi collegano telecamere tra soggetti diversi, sia pubblici che privati, o consentono la fornitura di servizi di videosorveglianza "in remoto" da parte di società specializzate (es. società di vigilanza, Internet providers) mediante collegamento telematico ad un unico centro.
- In tal caso sono obbligatorie **specifiche misure di sicurezza** (es. contro accessi abusivi alle immagini) e per alcuni sistemi è comunque necessaria la **verifica preliminare del Garante**.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- In particolare:
  - l'utilizzo condiviso di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, **l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando l'accesso a dati che esulano dalle competenze attribuite a ogni singolo ente**;
  - nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, **i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione**;
  - qualora la natura e le caratteristiche del sistema integrato siano tali da non consentire l'applicazione integrale di tali misure in ragione della natura dei dati o delle modalità del trattamento, è richiesta la verifica preliminare del Garante (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- In ogni caso qualora gli Enti locali intendano utilizzare sistemi "intelligenti" di videosorveglianza (basati ad esempio su software di riconoscimento facciale o su tecniche biometriche) gli stessi enti dovranno sottoporre al garante i sistemi per la verifica preliminare.
- Il Garante prescrive poi l'obbligo di adottare **specifiche cautele tecniche in caso di videosorveglianza tramite Internet o utilizzando tecnologie senza fili** (WiFi, WiMAX, GPRS), che si sostanziano nell'obbligo di **adozione di strumenti di identificazione e di protezione dei sistemi dalle intrusioni esterne** e, soprattutto dall'obbligo di utilizzare protocolli di cifratura nella trasmissione delle immagini a distanza.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

d. Deposito dei rifiuti

•In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad **accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi**.

•Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

e. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della Strada

- Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.
- **L'utilizzo di tali sistemi è quindi lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare**, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate.
- Le risultanze fotografiche o le riprese video rilevate **devono essere utilizzate solo per accertare le violazioni** delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;
- Le immagini devono essere conservate per il **periodo di tempo strettamente necessario in riferimento alla contestazione**, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- Al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.
- Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.
- Anche i conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle violazioni **devono essere previamente informati in ordine al trattamento dei dati personali**.
- Particolari disposizioni normative vigenti individuano talune ipotesi (come, ad es., in caso di rilevamento a distanza dei limiti di velocità) in cui **l'amministrazione pubblica è tenuta a informare gli utenti in modo specifico in ordine all'utilizzo di dispositivi elettronici.**

    - In tali casi è possibile fare a meno di fornire un'ulteriore, distinta informativa rispetto al trattamento dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale.

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

f. Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali

– Per gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio che **effettuano attività di videosorveglianza in forma integrata**,**tramite la compartecipazione ad un medesimo sistema di rilevazione**, l'Autorità Garante ha individuato un quadro di specifiche garanzie che i Comuni devono adottare in casi di sistemi integrati:

- l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da **permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti** istituzionali (evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente);

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

- nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati raccolti dovranno essere trattati in forma differenziata in relazione alle competenze istituzionali della singola pubblica amministrazione.

- Il titolare del trattamento è tenuto a richiedere una **verifica preliminare al Garante** in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure adottate e gli accorgimenti individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali il Provvedimento in esame la richiede espressamente (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

Provvedimento generale del Garante sulla videosorveglianza – 8 aprile 2010

g. PRESCRIZIONI E SANZIONI

– In caso di violazione delle misure necessarie prescritte dal Garante, il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all'**inutilizzabilità dei dati** personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);
- all'adozione di **provvedimenti di blocco o di divieto del trattamento** disposti dal Garante (*art. 143, comma 1, lett. c*), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- all'applicazione delle pertinenti **sanzioni amministrative o penali** (*artt. 161 e ss. del Codice*).

Altri riferimenti normativi

Circolare Ministero Interno - 6 agosto 2010 prot. N.558/A/421.2/70/195960

- Con la **Circolare del 6 agosto 2010**, il **Ministero dell'Interno** - Dipartimento della Pubblica Sicurezza ha sottolineato che:
  - *"appare importante rilevare come l'utilizzazione di sistemi di videosorveglianza per i luoghi pubblici o aperti al pubblico, qualora si profilino aspetti di tutela dell'ordine e della sicurezza pubblica, oltre a quelli di sicurezza urbana, possa determinare (..) l'affievolimento di alcuni principi di garanzia, quali, in particolare, quello dell'informativa".*
  - Il Ministero, richiamando la propria circolare del 8 febbraio 2005 avente ad oggetto la definizione di linee guida in materia di videosorveglianza, ribadisce che, **pur non essendo necessaria l'informativa per gli impianti comunali di videosorveglianza utilizzati anche per il controllo della sicurezza urbana e dell'ordine pubblico, è ad ogni modo opportuno che sia il Comitato Provinciale per l'Ordine e la Sicurezza ad esprimersi preventivamente**.

Circolare Ministero Interno
2 marzo 2012 - n. 588

- Il Ministero dell'Interno, attraverso la Circolare del 2 marzo 2012, ha fornito ulteriori riferimenti in merito all'adozione di impianti di videosorveglianza da parte dei Comuni.
- Negli aspetti giuridici viene segnalato di creare dei **Comitati di analisi della situazione della sicurezza urbana e di valutazione dell'opportunità o meno di installare impianti di videosorveglianza**.
- Si tratta dunque di un documento che, per la prima volta, non si limita a considerazioni di natura giuridica, ma offre anche una serie di indicazioni di natura tecnica: non basta decidere di installare un impianto di videosorveglianza, ma bisogna anche decidere dove le telecamere devono essere installate e quali devono essere i campi inquadrati.

Circolare Ministero Interno
2 marzo 2012 - n. 588

- Un altro problema affrontato dal Ministero, riguarda la circostanza che molti comuni, fra loro adiacenti, installano sistemi di videosorveglianza tra loro non compatibili, creando degli indubbi problemi (si pensi ad esempio a quando le forze dell'ordine devono ricostruire il percorso seguito da una macchina sospetta o da una macchina con rapinatori in fuga).
- L'opportunità di creare **sistemi** tra loro **compatibili**, per consentire una continuità di osservazione delle immagini tra la piattaforma installata da un comune e quella installata da un comune vicino, è indubbiamente raccomandabile.

Comitato Provinciale per l'Ordine e la Sicurezza Pubblica

- Il Comitato Provinciale per l'Ordine e la Sicurezza Pubblica (CPOSP) è organo consultivo del quale generalmente fanno parte
  - il Questore,
  - il Comandante Provinciale dei Carabinieri
  - il Comandante il Gruppo Guardia di Finanza.
- La composizione di tale organo è estendibile anche a soggetti esterni all'Amministrazione della Pubblica Sicurezza.
- I Comitati sono stati individuati dalle Circolari poc'anzi analizzate come le sedi idonee per esaminare:
  - la scelta delle aree,
  - le effettive esigenze che giustifichino il ricorso alle telecamere
  - l'attuazione di piani coordinati per il controllo del territorio.

Comitato Provinciale per l'Ordine e la Sicurezza Pubblica

- Più dettagliatamente, i Comitati svolgono attività valutative sui progetti di videosorveglianza futuri (da installare) quali:
  - tracciare un bilancio delle risorse umane e strumentali (ad esempio altri dispositivi esistenti) disponibili;
  - realizzare una “diagnosi locale” preliminare, ad esempio considerando:
    - la dimensione del contesto territoriale,
    - le condizioni di sicurezza del territorio (che devono essere peggiorative e caratterizzate da fenomeni non effimeri),
    - la possibilità di attuare strumenti di intervento alternativi alla videosorveglianza, così da dare maggiore sostanza al principio di necessità;
  - definire obiettivi e risultati attesi dall’impianto di videosorveglianza;
  - stabilire la tipologia del sistema che può rispondere agli obiettivi preposti;
  - verificare la corrispondenza del sistema prescelto alle caratteristiche tecniche che permettono trasferimento e conservazione ottimale delle immagini.

Le Linee Guida ANCI del 2010

Scuola Interregionale di Polizia
Locale

Premessa

- Le «**Linee Guida per i Comuni in materia di videosorveglianza alla luce del provvedimento Garante Privacy 8 aprile 2010**«, frutto della collaborazione dell'**Associazione Nazionale Comuni Italiani (ANCI)** con il **Garante della Privacy** sono finalizzate a "*fornire chiarimenti e strumenti di lavoro per una corretta applicazione, per quanto di competenza dei Comuni, circa l'utilizzo della videosorveglianza, anche ai fini della sicurezza urbana*".

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

FINALITA' :

•Il Garante per la protezione dei dati personali nel presente documento ha individuato, tra le finalità per l'utilizzo della videosorveglianza, quattro ambiti generali:

- **Protezione e incolumità degli individui**
- **Ordine e sicurezza pubblica, prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici**
- **Razionalizzazione e miglioramento dei servizi pubblici**
- **Protezione della proprietà di sedi, palazzi, biblioteche, musei e luoghi pubblici**.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

Il Garante ha riscontrato la necessità di sottoporre all'esame preventivo dell'Autorità l'installazione di qualsiasi impianto di videosorveglianza.

- **QUANDO OCCORRE L'ESAME PREVENTIVO DEL GARANTE**
  - Il Comune deve **sottoporre all'esame preventivo del Garante** solo ed esclusivamente i trattamenti di dati che intende effettuare mediante un impianto di videosorveglianza che:
    - Raccolga immagini associate a dati biometrici
    - Permetta il riconoscimento della persona tramite collegamento o tramite incrocio di immagine rilevate, con altri specifici dati personali, in particolare dati biometrici
    - Non si limiti a riprendere e registrare le immagini, ma sia in grado di rilevare comportamenti o eventi anomali, segnalarli e registrarli

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

QUANDO NON OCCORRE L'ESAME PREVENTIVO DEL GARANTE

- **Normali sistemi di videosorveglianza**
  - Il comune che intenda installare un sistema di videosorveglianza non deve sottoporlo all'esame preventivo del Garante, ma è sufficiente che il trattamento dei dati personali effettuato tramite tale tipo di impianto, avvenga previa informativa alle persone che stanno per accedere nell'aerea videosorvegliata.

  - **I sistemi integrati di videosorveglianza**
  - L'utilizzo di tali sistemi non deve essere sottoposto a verifica preliminare nei casi in cui possano essere applicate oltre le normali misure di sicurezza.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

- **I sistemi integrati di videosorveglianza per la sicurezza urbana nei comuni**
  - La videosorveglianza disposta per finalità di sicurezza urbana, non deve essere sottoposto a verifica preliminare qualora l'utilizzo condiviso di sistemi di videosorveglianza tramite la medesima infrastruttura sia configurato con modalità tali da permettere ad ogni singolo ente l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali.

    - **Durata della conservazione delle immagini**
  - I comuni possono conservare i dati registrati **fino a sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza**. E' opportuno precisare che non deve essere sottoposto ad una verifica preliminare del Garante l'esigenza di conservare le immagini anche oltre il periodo di una settimana qualora intervenga una specifica richiesta dell'autorità giudiziaria.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

- **Ulteriori casi di esclusione della verifica preliminare**
  - Non si deve richiedere la verifica preliminare purché siano rispettate le seguenti condizioni:
    - Il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti.
    - La fattispecie concreta, la finalità di trattamento, la tipologia di impiego del sistema che intende adottare corrispondono a quelle del trattamento approvato.
    - Si rispettino integralmente le misure e gli accorgimenti conosciuti o di concretamente conoscibili prescritti nel provvedimento di verifica preliminare

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

- Nel provvedimento, l'ANCI sottolinea l'estrema delicatezza nell'utilizzo di impianti di videosorveglianza dotati di sistemi di registrazione audio. Tali impianti inoltre incidono in maniera importante nella privacy dell'individuo, configurando una interferenza illecita nella vita privata, fattispecie che prevede sanzioni penali.

- Infatti solamente l'autorità giudiziaria può disporre registrazioni audio con tali sistemi, abbinati alle immagini di luoghi, locali e ambienti ben individuati.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

GESTIONE IMPIANTI VDS COMUNALI A BORDO DEI MEZZI PUBBLICI

•I sistemi di videosorveglianza spesso sono gestiti dai Comuni e dalle Aziende Municipalizzate di Trasporto Pubblico anche in base a specifici accordi con le locali Prefetture e Questure, nonché con le Forse dell'Ordine che possono ricevere anche in via diretta le immagini provenienti dai mezzi pubblici, in caso di allarme o emergenza.

•Sui mezzi di trasposto, l'ANCI ritiene che:

- Le immagini a bordo dei mezzi di trasporto pubblico non possono essere viste dal personale appartenente ai servizi di trasporto pubblico
- L'estrazione di immagini può essere effettuato solo dal personale autorizzato con delle credenziali
- Si deve garantire l'attività di registrazione dei log relativi alle attività di estrazione delle immagini.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

- È importante prestare la massima attenzione nel rispetto e nella tutela dei lavoratori a bordo dei mezzi di trasporto pubblico videosorvegliati, affinché lo strumento invasivo delle telecamere sia esclusivamente di prevenzione di atti criminosi e conseguente aumento della sicurezza del trasposto pubblico locale.

- **Per la videosorveglianza alle fermate del trasporto, L'ANCI inoltre ritiene che:**

  - Anche in questi casi esistono collegamenti diretti alle centrali operative con le Forze di Polizia dello Stato e delle Polizie Locali, con sistemi di estrapolazione delle immagini direttamente dalle forze dell'ordine.

  - La visione in diretta delle immagini potrà essere consentita anche al personale di Aziende Municipalizzate al fine di verificare in tempo reale le condizioni di afflusso alle varie fermate e monitorare eventuali criticità sui tempi di percorrenza.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

COLLEGAMENTI TRA CENTRALI FORZE DI POLIZIA E POLIZIA LOCALI

•Deve essere consentito ai comuni l'utilizzo di adeguati sistemi di videosorveglianza le cui immagini devono essere conservate e visionate in locali protetti gestiti dalle Polizie Locali, la cui estrapolazione deve avvenire sotto il controllo di personale qualificato delle medesime forze dell'ordine.

•Possono essere previsti collegamenti con le centrali Forze di Polizia dello Stato

•In un'ottica di collaborazione con le istituzioni di sicurezza, l'Anci ritiene che ogni installazione dei servizi di videosorveglianza da parte dei comuni debba passare l'esame preliminare del Comitato Provinciale e la Sicurezza Pubblica.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

- I comuni dovranno adottare tutte le cautele che vadano a prevenire eventuali forme di intrusione nella privacy dei cittadini.

- I comuni devono adottare ogni accorgimento volto ad evitare la ripresa di persone in abitazioni private, delimitando, la dislocazione, l'uso dello zoom ed in particolare l'angolo visuale delle telecamere, in modo da escludere ogni forma di ripresa.

- I comuni devono prestare particolare attenzione alla segnaletica e ai modelli di informativa che devono tassativamente informare, oltre alla finalità di sicurezza urbana, quelle di controllo e di conservazione delle immagini di propria competenza.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

- L'ufficio di Coordinamento della Polizia dello Stato, con una circolare, ha ricordato che ***«l'utilizzazione di sistemi di vds per i luoghi pubblici o aperti al pubblico, qualora si profili aspetti di tutela dell'ordine e della sicurezza pubblica, oltre a quelli di sicurezza urbana, possa determinare l'attrazione di tali apparecchiature nell'ambito delle previsioni dettate nel Provvedimento del Garante, con conseguente applicazione dell'art. 53 del Codice in materia di protezione dei dati personali e relativo affievolimento di alcuni principi di garanzia, quali in particolare, quello dell'informativa di cui all'art. 13 del cennato codice»***

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

PROCEDURE D'ACCESSO IMMAGINI

•Il Garante ricorda che tale operazione deve essere funzionale rispetto alla finalità di sicurezza urbana.

•L'Anci individua precisa finalità, ovvero le immagini potranno essere visionate:

- Sulla base di denunce di atti criminosi da parte dei cittadini, per il successivo inoltre delle fonti di prova all'autorità giudiziaria.
- Sulla base di segnalazioni relative ad atti criminosi accertate direttamente dagli organi di polizia in servizio sul territorio cittadino.
- Sulla base di atti criminosi che vengono rilevati direttamente dagli operatori di polizia nel visionare le immagini trasmesse in diretta dalle telecamere, nell'esercizio delle proprie funzioni.
- Sulla base di richieste specifiche per indagini dell'autorità giudiziaria
- Sulla base di ogni altra istanza delle autorità /organi che siano espressamente autorizzati secondo norme di legge.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

- Le immagini devono essere custodite in maniera protetta, in server dedicati e non su reti informatiche accessibili a tutti i dipendenti del comune.

- Il luogo ove è presente il server contenente le immagini deve essere accessibile solo mediante porta allarmante.

- L'accesso deve avvenire con la digitazione dei codici e chiava alfa numerica e gli uffici devono essere allarmati, nel caso di chiusura durante alcune ore della giornata.

- Nel caso in cui i server siano custoditi presso la centrale operativa della polizia locale, che l'accesso debba avvenire, ad esempio, attraverso videocitofono con l'identificazione immediata del dipendente autorizzato e di conseguenza impedire l'ingresso di personale non autorizzato

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

UTILIZZO VDS PER RILEVAZIONI DI VIOLAZIONI DEL CODICE DELLA STRADA

•La raccolta dei dati deve essere sempre pertinente e mai eccedente la finalità cui è preposto il titolare, senza invadere la sfera privata degli automobilisti, delimitando gli angoli di ripresa.

•In materia di controllo velocità dei veicoli vanno rammentate alcune disposizioni ministeriali:

- modalità di ripresa: le norme attuali in materia di controlli sui limiti di velocità e sui sorpassi, secondo il Regolamento di esecuzione e attuazione del Codice della Strada, attraverso dispositivi elettronici hanno trovato una puntuale applicazione con la Direttiva Ministero dell'Interno del 14/8/2009 prot. 300/A/10307/09/144/5/20/3 "*Direttiva per garantire un'azione coordinata di prevenzione e contrasto dell'eccesso di velocità sulle strade*", che ha definito molti aspetti relativi ai controlli e alla tutela della privacy.

Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento garante privacy 8 aprile 2010

SISTEMI DI RILEVAZIONE DEGLI ACCESSI DEI VEICOLI AI CENTRI STORICI E ZONE A TRAFFICO LIMITATO

•Sono numerosissimi i sistemi di videosorveglianza che controllano gli accessi alle Zone a Traffico Limitato, le Aree pedonali Urbane e le corsie riservate ai mezzi pubblici. In tal caso le attività sanzionatorie sono disposte dalla Polizia Locale.

- Tuttavia, non deve essere trascurato l'aspetto legato alla conservazione delle immagini scattate al momento della commessa violazione.

    - Tutte le immagini delle violazioni vanno custodite in appositi server, non connessi ad alcuna rete interna, accessibile solo al personale avente la qualifica di appartenente ad organo di polizia stradale (ufficiale o agente) o espressamente autorizzato con apposita nota riservata al personale di aziende esterne, che non svolgono funzioni di verbalizzazione.

PRINCIPALI SANZIONI AMMINISTRATIVE

L'ANCI richiama l'attenzione di tutte le amministrazioni comunali riguardo le possibili sanzioni sia penali che amministrative, queste ultime particolarmente onerose, in cui potrebbero incappare i comuni, a seguito di visite ispettive dello specifico Nucleo Tutela Privacy del Garante per la Protezione dei Dati Personali o a seguito di segnalazioni dei cittadini, che ritengono lesa la propria riservatezza. Qui di seguito si indicano le principali sanzioni amministrative e penali:

NORMA E TIPO D'INFRAZIONE	SANZIONE EDITTALE	PAGAMENTO IN MISURA RIDOTTA - DESTINAZIONE PROVENTI - AUTORITÀ COMPETENTE A RICEVERE IL RAPPORTO E AD IRROGARE LE SANZIONI	NOTE/OSSERVAZIONI
Omissione o inidoneità dell'informativa (es. laddove non è indicato il titolare del trattamento o la finalità perseguita) **Artt. 13 e 161 del Codice**	Sanzione amm.va da 6.000 € a 36.000 €	• 12.000 € entro 60 gg • Stato • Garante	v. punto 3.1 Provv. Garante dell'08/04/10 (Informativa)
Mancata o incompleta notificazione del trattamento dei dati personali al Garante **Artt. 37, 38 e 163 del Codice**	Sanzione amm.va da 20.000 € a 120.000 €	• 40.000 € entro 60 gg • Stato • Garante	v. punto 3.2 Provv. dell'08/04/10 (Prescrizioni specifiche). La violazione ricade su chiunque sia tenuto ad osservare tale prescrizione
Inosservanza dei provvedimenti di prescrizione di misure necessarie **Art. 162, comma 2-ter, del Codice**	Sanzione amm.va da 30.000 € a 180.000 €	• 60.000 € entro 60 gg • Stato • Garante	v. punto 3.3.1. nelle lettere da a) ad f) Provv. dell'08/04/10 (Misure di sicurezza)

PRINCIPALI SANZIONI AMMINISTRATIVE

NORMA E TIPO D'INFRAZIONE	SANZIONE EDITTALE	PAGAMENTO IN MISURA RIDOTTA - DESTINAZIONE PROVENTI - AUTORITÀ COMPETENTE A RICEVERE IL RAPPORTO E AD IRROGARE LE SANZIONI	NOTE/OSSERVAZIONI
Omessa adozione di misure minime di sicurezza **Artt. 33 e 162, comma 2-bis del Codice**	Sanzione amm.va da 10.000 € a 120.000 €	• Non è ammesso il p.m.r. • Stato • Garante	Tale violazione integra la fattispecie del reato ex art. 169 del Codice (Misure di sicurezza), che punisce con l'arresto fino a 2 anni, chi omette di adottare le prescritte misure di sicurezza. v. punto 3.3.2. Provv. dell'08/04/10 (Responsabili e incaricati)
Mancato rispetto dei tempi di conservazione delle immagini raccolte e collegato obbligo di cancellazione di delle immagini oltre il termine previsto **Art. 162, comma 2-ter, del Codice**	Sanzione amm.va Da 30.000 € a 180.000 €	• 60.000 € Entro 60 gg; • Stato • Garante	v. punto 3.4 Provv. dell'08/04/10
Omessa informazione o esibizione di documenti al garante Artt. 157 e 164, del Codice	Sanzione amm.va 10.000 € a 60.000 €	• 20.000 € Entro 60 gg; • Stato • Garante	La violazione ricade su chiunque sia tenuto ad osservare tale prescrizione

Illeciti penali

IPOTESI DI REATO	SANZIONI PREVISTE	AUTORITÀ COMPETENTE	NOTE/OSSERVAZIONI
TRATTAMENTO ILLECITO DI DATI			
Trattamento illecito di dati personali da parte di soggetti pubblici (salvo che il fatto non costituisca più grave reato) Art. 167, comma 1 del Codice (1^ Ipotesi)	Se ne deriva un danno: Reclusione da 6 mesi a 18 mesi; In caso comunicazione o diffusione dei dati: Reclusione da 6 mesi a 24 mesi	Procura della Repubblica presso il Tribunale Garante	Il fine è quello di trarre per sé o altri profitto o di recare ad altri un danno. Cfr. Artt. 18 e 19 del Codice
Trattamento illecito di dati personali da parte di soggetti pubblici (salvo che il fatto non costituisca più grave reato) Art. 167, comma 2 del Codice (2^ Ipotesi)	Se ne deriva un danno: Reclusione da 1 a 3 anni	Procura della Repubblica presso il Tribunale Garante	Il fine è quello di trarre per sé o altri profitto o di recare ad altri un danno. Cfr. Artt. 17, 20, 21, 22 c.c. 8 e 11, e 45 del Codice
FALSITÀ NELLE DICHIARAZIONI O NOTIFICAZIONI			
Chiunque dichiari o attesti falsamente notizie o circostanze o produce atti o documenti falsi (salvo che il fatto costituisca più grave reato) Art. 168, comma 1 del Codice	Reclusione da 6 mesi a 3 anni	Procura della Repubblica presso il Tribunale Garante	Es. falsità nella notificazione del trattamento ex art. 37 del Codice, o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti

Illeciti penali

IPOTESI DI REATO	SANZIONI PREVISTE	AUTORITÀ COMPETENTE	NOTE/OSSERVAZIONI
MISURE DI SICUREZZA			
Chiunque, essendovi tenuto, omette di adottare le misure minime di sicurezza. Art. 169, comma 1 del Codice	Arresto sino a 2 anni (reato contravvenzionale)	Procura della Repubblica presso il Tribunale Garante	v. Art. 33 del Codice Il c. 2 dell'art. 169 prevede una regolarizzazione entro un termine fissato dal Garante che estingue il reato (adempimento della prescrizione e pagamento di una sanzione amm.va. di 45.000 €, entro 6 mesi).
INOSSERVANZA DI PROVVEDIMENTI DEL GARANTE			
Chiunque, essendovi tenuto, non osserva il provvedimento del Garante Art. 170, comma 1 del Codice	Reclusione da 3 mesi a 2 anni	Procura della Repubblica presso il Tribunale Garante	v. artt. 150 c.c. 1 e 2, e 143, c. 1 lett. c) del Codice
PENE ACCESSORIE			
La condanna per uno dei delitti previsti dal D.Lgs. nr. 196 del 2003, prevede la pubblicazione della sentenza (art. 172 del Codice).			

Schema di regolamento per la disciplina della videosorveglianza nei territori comunali

- I Comuni che adottano dispositivi di videosorveglianza devono predisporre uno specifico regolamento al fine di disciplinare dettagliatamente tutti gli aspetti della materia. Di seguito lo schema di regolamento fornito dal Garante**:**

❖ **INDICE**

- **CAPO I PRINCIPI GENERALI**
  - Art. 1 – Oggetto
  - Art. 2 - Definizioni
  - Art. 3 - Finalità
  - Art. 4 - Trattamento dei dati personali
- **CAPO II OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO**
  - Art. 5 - Notificazione
  - Art. 6 - Responsabile
  - Art. 7 - Persone autorizzate ad accedere alla sala di controllo
  - Art. 8 - Nomina degli incaricati e dei preposti gestione dell'impianto di videosorveglianza
  - Art. 9 - Accesso ai sistemi e parola chiave

Schema di regolamento per la disciplina della videosorveglianza nei territori comunali

- **CAPO III TRATTAMENTO DEI DATI PERSONALI**
  - **Sezione I – Raccolta e requisiti dei dati personali**
    - Art. 10 - Modalità di raccolta e requisiti dei dati personali
    - Art. 11 - Obbligo degli operatori
    - Art. 12 - Informazioni rese al momento della raccolta
  - **Sezione II – Diritti dell'interessato nel trattamento dei dati**
    - Art. 13 - Diritti dell'interessato
  - **Sezione III – Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento dei danni**
    - Art. 14 - Sicurezza dei dati
    - Art. 15 - Cessazione del trattamento dei dati
    - Art. 16 - Limiti alla utilizzazione di dati personali
    - Art. 17 - Danni cagionati per effetto del trattamento di dati personali
  - **Sezione IV – Comunicazione e diffusione dei dati**
    - Art. 18 - Comunicazione

Schema di regolamento per la disciplina della videosorveglianza nei territori comunali

- **CAPO IV TUTELA AMMINISTRATIVA E GIURISDIZIONALE**
  - Art. 19 - Tutela
- **CAPO V MODIFICHE**
  - Art. 20 - Modifiche regolamentari

Carta per un utilizzo democratico della videosorveglianza

- La **Carta per un utilizzo democratico della videosorveglianza** è un documento che disciplina, mediante raccomandazioni, l'elaborazione, il funzionamento e lo sviluppo di sistemi di videosorveglianza pubblici, gestiti da autorità pubbliche, siano esse statali, regionali, provinciali o locali.
- Il documento, elaboratpo nell'ambito del progetto europeo denominato «*Citizens, cities and video surveillance» (*realizzato dal Forum Europeo sulla Sicurezza Urbana – FESU - in collaborazione con 6 città partner - Genova, Ibiza, Le Havre, Saint-Herblain, Liegi,Rotterdam - e altri soggetti -Regione Emilia Romagna, Regione Veneto, London Metropolitan Police e la Polizia del Sussex -), concluso nel 2010, persegue l'obiettivo di promuovere un uso efficace della videosorveglianza e fornire elementi di conoscenza e consapevolezza nella gestione della videosorveglianza che consentano agli Enti locali di adottare strategie locali che offrano ai propri cittadini maggiore sicurezza salvaguardando però il loro diritto alla riservatezza.

Carta per un utilizzo democratico della videosorveglianza

- La Carta **non costituisce assolutamente un documento normativo**; essa prova solo a contemperare le esigenze delle città nell'elaborazione e funzionamento dei dispositivi di videosorveglianza e, dall'altra, il bisogno dei cittadini di avere garanzie nell'impiego di tali sistemi.
- Attraverso l'adesione alla Carta le città firmatarie si sono impegnate a rispettare i principi enucleati nel documento (liceità, necessità, proporzionalità, trasparenza, responsabilità, supervisione indipendente, coinvolgimento dei cittadini), nonchè a dare attuazione alle misure concrete e alle raccomandazioni riguardanti l'adozione e l'operatività dei dispositivi tecnologici (necessità di effettuare una diagnosi locale preliminare all'installazione delle telecamere, valutazioni periodiche del sistema, formazione degli operatori)
- Le norme che enuncia possono essere applicate anche a sistemi di videosorveglianza privati, in particolare quando l'esercizio di tali impianti può essere devoluto alle autorità pubbliche.

Sistemi di sicurezza integrata

Piani coordinati di controllo

- L'art. 6 del d.l. 23 maggio 2008, n. 92, consente ai **Comuni diversi da quelli dei maggiori centri urbani di realizzare Piani coordinati di controllo del territorio**, anche per specifiche esigenze, determinando così rapporti di reciproca collaborazione fra il personale della Polizia municipale e provinciale e gli organi di Polizia dello Stato.
- La stessa legge, all'art. 7, demanda ad un decreto del Ministro dell'Interno l'individuazione delle procedure da osservare per assicurare, nel corso dello svolgimento dei piani coordinati di controllo del territorio, le modalità di raccordo operativo tra la Polizia municipale, la Polizia provinciale e gli organi di Polizia dello Stato.
- Si consideri che l'impegno degli Enti locali nella gestione della sicurezza urbana, inoltre, è vincolato a forme di collaborazione strutturale ed operativa con le amministrazioni statali, per espressa riserva costituzionale (art. 117, lett. H, Cost.).

Piani coordinati di controllo

- Negli ultimi anni si è assistito ad una crescente diffusione, nelle realtà locali minori, di questi Piani coordinati di controllo, raggiunti mediante **sottoscrizione di specifici patti**, è stata oggetto di numerosi accordi tra gli Enti Locali per garantire nel migliore dei modi la sicurezza delle rispettive comunità.
- I patti per la sicurezza hanno portato le autonomie locali a sviluppare un **sistema di sicurezza integrato**, con il concorso di soggetti diversi nella progettazione e realizzazione delle politiche per la sicurezza, ciascuno con la propria specificità.
- I soggetti coinvolti sono:
  - le amministrazioni locali, con azioni di prevenzione e di inclusione sociale,
  - le Forze dell'ordine con azioni di contrasto e repressione,
  - la cittadinanza con l'offerta di collaborazione e di informazione.

- Si è così andato affermando il concetto di "**sicurezza condivisa**", "p**artecipata**", "i**ntegrata**", sotto il controllo ed il governo degli apparati statali, centrali e periferici.

Sicurezza pubblica e privata

- L'art. 118 della Costituzione afferma che «*Stato, Regioni, Città metropolitane, Province e Comuni favoriscono l'**autonoma iniziativa dei cittadini, singoli e associati**, per lo svolgimento di attività di interesse generale, sulla base del principio di sussidiarietà*»

- L'art. 1 del T.U.L.P.S., nell'affermare la competenza statale nella gestione dell'ordine e della sicurezza pubblica, nonché nella garanzia dell'incolumità dei cittadini e della tutela dei loro beni, **non impedisce ad altri soggetti, pubblici e privati, di operare e collaborare per gli stessi fini**.

- Alla luce di tali disposizione, nel corso degli anni, in considerazione della difficoltà sempre crescente di far fronte all'esigenza di tutela della collettività, molteplici sono stati gli accordi tra enti locali e soggetti privati per disciplinare il loro concorso in alcune attività (c.d. "sussidiarie") volte a garantire la sicurezza dei cittadini.

Sicurezza integrata e sussidiaria

- Ciò ha contribuito alla nascita della c.d. **sicurezza "integrata**", quale strumento attuativo di politiche che vedono integrarsi le competenze esclusive dello Stato in materia di ordine e sicurezza pubblica, con quelle riconducibili agli enti locali ed ai privati operanti sul piano della prevenzione, quali governi territoriali di prossimità.

- La **sicurezza "sussidiaria**" indica, dunque, l'insieme delle varie attività, poste in essere professionalmente da soggetti privati (singoli od associati), integrative o complementari della sicurezza approntata dalle forze di polizia.

Sicurezza integrata e sussidiaria

- La possibilità per i privati di assumere in sussidiarietà una funzione pubblica, dipende:
  - dalla natura dell'attività da svolgere,
  - dalla capacità di dar vita ad un sistema adeguato che consenta di contemperare le esigenze della sicurezza con la garanzia dei cittadini.
- L'utilizzo del termine sussidiarietà è stato scelto al fine di evidenziare il carattere complementare delle attività sopra citate, rispetto alle funzioni di **sicurezza "primaria**" che restano affidate alle forze di polizia.
- Lo svolgimento delle attività di sicurezza "sussidiaria" presuppone che **non vengano esercitate pubbliche funzioni, o svolti compiti comunque riservati alle forze di polizia**.
  - Con il DPR 153/2008 è stato introdotta una nuova nozione per la qualificazione dei servizi di vigilanza svolti dalle guardie particolari giurate: il concetto di **sicurezza complementare,** a significare che **si tratta di sicurezza aggiuntiva, accessoria ed integrativa rispetto alla "attività" di Pubblica sicurezza in senso stretto, svolta dalle forze di polizia**.

Sicurezza integrata e sussidiaria

- La sicurezza integrata e sussidiaria, è stata attuata attraverso la collaborazione con differenti figure:
  - volontari cui è stata riconosciuta la qualifica di agente di Pubblica sicurezza (ad es. i barracelli, che pur non essendo pubblici dipendenti, per le funzioni svolte nell'ambito del territorio di competenza, rivestono, a seguito di decreto prefettizio, la qualifica di agenti di Pubblica sicurezza);
  - i volontari cui è stata riconosciuta la qualifica di incaricato di pubblico servizio (in presenza di una situazione nella quale il volontario coopera nella gestione di un "servizio di Pubblica sicurezza", esso viene a svolgere un pubblico servizio, inserito ed inquadrato nell'Amministrazione della Pubblica sicurezza);
  - lavoratori dipendenti cui è stata riconosciuta la qualifica di incaricato di pubblico servizio (guardie particolari giurate; steward; personale addetto ai servizi di controllo delle attività di intrattenimento e di spettacolo in luoghi aperti al pubblico o in pubblici esercizi);
  - lavoratori dipendenti sprovvisti di una qualifica pubblica (il personale della security aziendale, che si occupa dello studio, sviluppo ed attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa che possono danneggiare le risorse materiali, immateriali, organizzative e umane di cui l'azienda dispone o di cui necessita per garantirsi una adeguata capacità di sviluppo nel breve, nel medio e nel lungo termine).

Sicurezza integrata e sussidiaria.
Le guardie giurate e istituti di vigilanza

Scuola Interregionale di Polizia
Locale

Le guardie giurate e gli istituti di vigilanza

- L'attività di vigilanza privata è disciplinata dal titolo IV del T.U.L.P.S., che prevede possa essere svolta secondo due diverse modalità:
  - ai sensi dell'art. 133 T.U.L.P.S., **sono gli stessi proprietari a poter direttamente impiegare propri dipendenti riconoscendo loro il ruolo di guardie giurate deputate allo svolgimento di attività di vigilanza e custodia dei beni**;
  - ai sensi dell'art. 134 T.U.L.P.S., **l'attività di vigilanza può essere svolta, previa autorizzazione prefettizia, da persone giuridiche private o singole persone fisiche che impieghino propri dipendenti, in via professionale ed in forma imprenditoriale, riconosciuti come guardie giurate, al servizio a richiesta di proprietari di beni**.
- In sostanza, **l'attività delle guardie giurate consiste nell'esercitare l'attività di vigilanza o di custodia di beni mobili o immobili altrui, sia direttamente alle dipendenze di enti** (pubblici o collettivi) **o di privati proprietari** (singoli o associati), **sia indirettamente alle dipendenze di istituti di vigilanza**.

Le guardie giurate e gli istituti di vigilanza

- L'esercizio dell'attività disciplinata dall'art. 134 T.U.L.P.S. è subordinata al rilascio di una **specifica autorizzazione da parte del prefetto**, che, come tutte le autorizzazioni di polizia, è rilasciata *intuitu personae*: essa è strettamente personale e, pertanto, intrasmissibile, né cedibile neanche in rappresentanza. Ne discende che, ove anche il titolare della licenza nomini di propria iniziativa un dipendente quale procuratore o direttore, tale investitura esplica i propri effetti solo tra le parti.

- Il potere di controllo prefettizio inerisce non solo la fase genetica del rilascio (o del diniego) della licenza, ma anche la fase funzionale, in relazione alle modalità in cui l'attività sarà svolta.

- Un'ulteriore facoltà di controllo pubblico esercitabile sugli istituti di vigilanza o anche direttamente sulle guardie giurate è regolamentata dall'art. 139 T.U.L.P.S che prevede, da un lato, che gli istituti di vigilanza sono tenuti a prestare la loro opera a richiesta delle autorità di pubblica sicurezza e, dall'altro, che anche le stesse guardie giurate devono assolvere i compiti loro direttamente impartiti su iniziativa di ufficiali o agenti appartenenti alle forze dell'ordine.

Le guardie giurate e gli istituti di vigilanza

- Qualsiasi variazione abbia ad oggetto il funzionamento dell'istituto di vigilanza necessita di una **ulteriore autorizzazione da parte del prefetto**; il titolare dell'istituto deve:
  - comunicare al prefetto gli elenchi del personale dipendente,
  - dare notizia di ogni variazione intervenuta nel corso del rapporto,
  - restituire i decreti di nomina delle guardie giurate quando abbiano cessato di prestare servizio,
  - fornire gli opportuni riferimenti e generalità dei loro clienti/committenti, al fine di favorire un proficuo coordinamento con l'azione delle forze di polizia.
- L'**esercizio abusivo dell'attività di vigilanza**, in difetto della licenza prefettizia, è reato sancito dall'art. 140 T.U.L.P.S : «I contravventori alle disposizioni di questo titolo sono puniti con l'arresto fino a due anni e con l'ammenda da € 206,00 ad € 619,00».
- Circa l'ambito territoriale entro cui l'istituto di vigilanza può esercitare le proprie funzioni, **nella licenza deve esser fatta menzione dei comuni e delle località in cui l'attività può essere svolta**.

Le guardie giurate e gli istituti di vigilanza

- **Requisiti** (art. 138 T.U.L.P.S.)
  - essere cittadino italiano o di uno Stato membro dell'Unione europea;
  - avere raggiunto la maggiore età ed avere adempiuto agli obblighi di leva;
  - sapere leggere e scrivere;
  - non avere riportato condanna per delitto;
  - essere persona di ottima condotta politica e morale;
  - essere munito della carta di identità;
  - essere iscritto alla cassa nazionale delle assicurazioni sociali e a quella degli infortuni sul lavoro.

- Le guardie particolari giurate, inoltre, possono conseguire la licenza di porto d'armi.

Le guardie giurate e gli istituti di vigilanza

- **Rientrano nei servizi di sicurezza complementare, da svolgersi a mezzo di guardie particolari giurate, salvo che la legge disponga diversamente o vi provveda la forza pubblica, le attività di vigilanza concernenti:**
  - la sicurezza negli aeroporti, nei porti, nelle stazioni ferroviarie, nelle stazioni delle ferrovie metropolitane e negli altri luoghi pubblici o aperti al pubblico specificamente indicati dalle norme speciali, ad integrazione di quella assicurata dalla forza pubblica;
  - la custodia, il trasporto e la scorta di armi, esplosivi e di ogni altro materiale pericoloso, nei casi previsti dalle disposizioni in vigore o dalle prescrizioni dell'autorità, ferme restando le disposizioni vigenti per garantire la sicurezza della custodia, del trasporto e della scorta;
  - la custodia, il trasporto e la scorta del contante o di altri beni o titoli di valore; nonché la vigilanza nei luoghi in cui vi è maneggio di somme rilevanti o di altri titoli o beni di valore rilevante, appartenenti a terzi;
  - la vigilanza armata mobile e gli interventi sugli allarmi, salve le attribuzioni degli ufficiali e agenti di pubblica sicurezza;
  - la vigilanza presso infrastrutture del settore energetico o delle telecomunicazioni, dei prodotti ad alta tecnologia, di quelli a rischio di impatto ambientale, ed ogni altra infrastruttura che può costituire, anche in via potenziale, un obiettivo sensibile ai fini della sicurezza o dell'incolumità pubblica o della tutela ambientale.
  - Rientra altresì nei servizi di sicurezza complementare la vigilanza presso tribunali ed altri edifici pubblici, installazioni militari, centri direzionali, industriali o commerciali ed altre simili infrastrutture, quando speciali esigenze di sicurezza impongono che i servizi medesimi siano svolti da guardie particolari giurate.

Le guardie giurate e gli istituti di vigilanza

Qualifica di pubblici ufficiali

•Quello relativo all'esatta natura, pubblicistica o privatistica, da attribuire all'attività espletata dalle guardie giurate è un tema piuttosto controverso: al quadro normativo di non facile lettura si sono sovrapposti due diversi orientamenti giurisprudenziali e dottrinali tra loro in aperto contrasto.

•Attribuire natura pubblica all'attività espletata dalle guardie giurate significa, innanzitutto, attribuire o negare ad esse lo status giuridico di pubblico ufficiale.

•La prevalente giurisprudenza aderisce alla **tesi pubblicistica**, rinvenendone il fondamento normativo nel combinato disposto degli artt. 133 e ss. T.U.L.P.S. e dell'art. 255 del relativo regolamento di esecuzione. Tale orientamento affermando altresì che le guardie giurate, nell'ambito delle loro specifiche mansioni, svolgono attività di polizia giudiziaria e che, pertanto, **sono da considerarsi pubblici ufficiali**.

Le guardie giurate e gli istituti di vigilanza

Qualifica di pubblici ufficiali

•L'attribuzione alle guardie giurate della qualifica di pubblico ufficiale, inoltre, secondo parte della giurisprudenza, non discende dal rilascio all'istituto di vigilanza presso cui dipendono della licenza, poiché detta qualifica dipende esclusivamente dal concreto esercizio delle funzioni di prevenzione e repressione cui le guardie giurate sono preposte.

- Tale assunto deriva dal principio secondo cui sono ufficiali ed agenti di polizia giudiziaria, nei limiti del servizio a cui sono destinate e secondo le attribuzioni ad esse conferite dalle leggi e dai regolamenti, tutte le persone incaricate di svolgere compiti di prevenzione e repressione di determinate specie di reati. Le guardie giurate sono, infatti, chiamate allo svolgimento di tali compiti avendo ricevuto specifica investitura amministrativa all'esercizio di poteri che attengono alla potestà dello Stato: pertanto, nei limiti delle loro competenze, al pari degli organi di polizia giudiziaria, anche le guardie giurate sono chiamate, come pubblici ufficiali, ad agire in nome e per conto dello Stato.

Le guardie giurate e gli istituti di vigilanza

Qualifica di pubblici ufficiali

•In contrasto con le posizioni fino ad ora espresse, la giurisprudenza degli anni novanta che ha invece riconosciuto alla guardia giurata la **qualifica di incaricato di pubblico servizio e non di pubblico ufficiale**, sulla base del dettato dell'art. 358 c.p., il quale, al primo comma, indica come incaricati di pubblico servizio coloro i quali prestano a qualunque titolo un pubblico servizio e, al comma successivo, afferma che per pubblico servizio si debba intendere "*un attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*".

Protocolli d'intesa

- I Comuni sempre più spesso affidano ad istituti di sorveglianza privati i controlli per contrastare i reati mediante la conclusione di specifici accordi noti come «Protocolli d'intesa».
- Un esempio è costituito dal Protocollo "Mille Occhi sulle Città", siglato l'11 febbraio 2010 tra Ministero dell'Interno, ANCI e le organizzazioni rappresentative degli istituti di vigilanza il quale indica, insieme alle procedure da seguire per l'effettiva applicazione sul territorio, le forme che questa collaborazione può assumere.
  - In concreto, al verificarsi di una delle situazioni contemplate, la guardia giurata deve tempestivamente allertare, secondo le modalità apprese durante la formazione, la centrale operativa dell'istituto di vigilanza individuato come punto di raccolta di queste comunicazioni, che a sua volta è connessa alle sale operative delle forze di polizia di Stato e locali.
  - Il Protocollo elenca in dettaglio quali casi debbano sollecitare l'attenzione delle guardie giurate e diventare oggetto di allerta, tra essi, a titolo esemplificativo, si ricordano: la presenza di mezzi di trasporto o di persone sospette; l'eventuale fuga di mezzi o persone dal luogo del delitto; la segnalazione di ogni situazione che faccia ritenere imminente la commissione di reati, etc..)

Protocolli d'intesa

- I firmatari del protocollo hanno concordato che il contributo delle guardie giurate alla vigilanza sul territorio è corollario della più generale attività di vigilanza e per questo motivo non comporta l'esercizio di pubbliche funzioni e non può comportare costi od oneri ulteriori rispetto a quelli corrisposti dalla committenza all'Istituto di vigilanza privata per i servizi espletati.
- L'attuazione del Protocollo non è automatica ma ha richiesto alcuni passaggi a livello locale da parte della Prefettura, snodo nevralgico del Ministero dell'Interno a livello locale:
  - ai Prefetti è stato attribuito l'incarico di individuare gli Istituti di vigilanza privata da coinvolgere nel progetto, utilizzando come criteri di selezione le dotazioni tecnologiche, il numero di guardie giurate impiegate ed i servizi svolti. Una volta sentito il parere del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica - e d'intesa con i Comuni per gli aspetti relativi alla sicurezza urbana - i Prefetti hanno proceduto alla stipula delle convenzioni.
  - i Questori hanno invece predispostole modalità operative, tenendo anche in conto le specificità locali.

Gestori Outsourcing

- Il Garante, ammettendo la creazione di sistemi integrati pubblici di videosorveglianza ad opera degli Enti locali, implicitamente consente a tali Enti di affidare la gestione delle telecamere anche a soggetti esterni.
- Tali attività devono tuttavia essere circondate di cautele che si riassumono essenzialmente nella tracciabilità
  - degli accessi del personale,
  - del requisito dell'identificazione specifica di chi ha accesso ai sistemi,
  - dell'impossibilità di ricostruire percorsi dei singoli cittadini all'interno del territorio comunale.
- Qualora il sistema di videosorveglianza venga gestito da una società outsourcing la responsabilità nel trattamento dei dati sarà in capo alla medesima.
  - Per l'intera durata della concessione il Gestore potrà essere individuato come incaricato del trattamento dati e dovrà garantire lo svolgimento di tutte le attività inerenti il servizio erogato nel pieno rispetto della normativa vigente in materia di privacy e videosorveglianza.

Casi Pratici

Casi pratici

- Un’associazione di risparmiatori e consumatori si è rivolta all’Autorità segnalando l’installazione delle telecamere da parte di un comune che intendeva monitorare le operazioni di smaltimento dei rifiuti per verificare che venissero rispettate le disposizioni sulla raccolta differenziata.
  - **Il Garante ha ribadito che non è lecito utilizzare sistemi di videosorveglianza solo per accertare eventuali violazioni amministrative derivanti dal mancato rispetto delle disposizioni su modalità e orari di deposito dei sacchetti dei rifiuti dentro gli appositi contenitori**.

(*Newsletter Garante Protezione per i dati personali n. 246 del 21 - 27 febbraio 2005*)

Casi pratici

- Il Garante, su richiesta del Ministero dell'Interno in ordine a due schemi di decreto interministeriale sulla **registrazione di immagini** e sul rilascio di titoli di ingresso presso alcuni impianti sportivi in cui si svolgono incontri di calcio, ha promosso il sistema di videosorveglianza, sottolineando che "*l'introduzione della videosorveglianza presso impianti sportivi di capienza superiore alle diecimila unità, in occasione di competizioni calcistiche, (…) rispetta (…) il principio di liceità" (art. 11, comma 1, lett. a), del Codice "è altresì giustificata alla luce del principio di necessità nel trattamento dei dati, in ragione dei reiterati disordini e degli episodi di violenza verificatisi anche in epoca recente (art. 3 del Codice)".*

Casi pratici

Videosorveglianza di luoghi pubblici da parte di persone private

•**In linea generale, alla luce delle regole esaminate, non è ammesso per principio che persone private attivino un impianto di videosorveglianza su suolo pubblico.**

- *Esempio:* Il proprietario di una casa constata ripetutamente che il suo immobile subisce danni materiali causati da passanti e vorrebbe perciò sottoporre a videosorveglianza la strada antistante.

•Un impianto di videosorveglianza che controlli luoghi pubblici per tutelare interessi privati riprende un numero indefinito di persone ledendo in tal modo i loro diritti della personalità. Spesso gli interessati non hanno infatti alcuna possibilità di scegliere se entrare o meno nell'area sorvegliata e sono perciò costretti a esporsi a quest'ingerenza. Interessi privati non possono giustificare una situazione del genere.

•**Mantenere la sicurezza e l'ordine nei luoghi pubblici non compete ai privati, ma rientra nei compiti delle forze di polizia.**

Casi pratici

Videosorveglianza di luoghi pubblici da parte di persone private

•Eccezioni ipotizzabili a questa regola:

– Un Comune potrebbe accettare per motivi di praticità che un privato, nel **rispetto delle regole dettate dal Garante Privacy**, installi un sistema (legittimo) di videosorveglianza su un proprio terreno riprendendo anche suolo pubblico, in misura molto limitata, se **non è possibile sorvegliare altrimenti l'area privata**.

- *Esempio*: una banca installa vicino a un bancomat una videocamera che, oltre al bancomat, riprende anche una piccola parte di marciapiede. Dato che la sorveglianza del bancomat presuppone un interesse privato preponderante e non potrebbe avvenire senza riprendere parte del marciapiede, **potrebbe** essere ammessa.

Casi pratici

Videosorveglianza di luoghi pubblici da parte di persone private

- Una persona privata desidera sorvegliare suolo pubblico per ragioni di sicurezza contatta le autorità pubbliche competenti con cui concorda di effettuare lei stessa le necessarie misure di videosorveglianza o di integrare quelle che già effettuano loro sul medesimo suolo.
- Dato che disciplinare la videosorveglianza in ambito pubblico è di competenza dei Comuni, occorre chiarire previamente con le autorità se un accordo di questo tipo è ammesso.
- Recentemente, nell'ottica di potenziare e migliorare il sistema di videosorveglianza, alcuni Comuni hanno concluso accordi con privati o con altri Enti Locali aventi ad oggetto la condivisione delle spese di acquisto per l'installazione di telecamere di videosorveglianza.

  - *Esempio*: Il Comune di Loano ha concluso un accordo con privati (gestori delle giostre sul lungomare di Loano) concedendo loro di collegarsi al sistema di videosorveglianza comunale (a tutela delle giostre e dello spazio pubblico limitrofo), a fronte del lor contributo economico all'installazione di telecamere.

Verifica preliminare richiesta da Comune di Bergamo – 21 marzo 2013

- Il Comune di Bergamo ha presentato al Garante Privacy una richiesta di verifica preliminare, ai sensi dell'art. 17 del Codice, con riferimento al trattamento di dati personali effettuato mediante un sistema di videosorveglianza intelligente che intendeva installare, nel «*contesto delle politiche di sicurezza»*, presso taluni edifici monumentali e sedi istituzionali.

- Più precisamente, il trattamento di dati personali sottoposto a verifica preliminare dal Comune riguardava l'utilizzo di un sistema di videosorveglianza che prevedeva l'attivazione di un sistema di allarme idoneo a rilevare in tempo reale la sosta di un soggetto, per un determinato periodo di tempo, all'interno di un'area delimitata da una linea di interdizione virtuale in prossimità di sedi e edifici selezionati, al fine di garantire ad essi adeguata sicurezza sotto il profilo della prevenzione e tutela da azioni criminose, vandaliche e danneggiamenti.

Verifica preliminare richiesta da Comune di Bergamo – 21 marzo 2013

- Secondo il Garante:
  - Il trattamento di dati personali attraverso un sistema di videosorveglianza deve essere svolto nel rispetto delle disposizioni contenute nel Codice e delle indicazioni fornite dal Garante nel provvedimento generale in materia di videosorveglianza dell'8 aprile 2010;
  - Il titolare è tenuto a richiedere una verifica preliminare in tutti i casi in cui i trattamenti che intende effettuare tramite sistemi di videosorveglianza comportino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare (art. 17 del Codice) ed in particolare con riferimento ai sistemi di videosorveglianza c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed, eventualmente, registrarli.
  - l'utilizzo dei predetti sistemi risulta giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza

Verifica preliminare richiesta da Comune di Bergamo – 21 marzo 2013

- Il sistema di videosorveglianza sottoposto alla verifica del Garante, in concreto, non comportava un pregiudizio rilevante per l'interessato, idoneo a determinare effetti particolarmente invasivi sulla sua sfera di autodeterminazione e, più in generale, sui suoi diritti e libertà fondamentali.
- Le caratteristiche specifiche del sistema in esame, infatti, nel rilevare la presenza prolungata dell'interessato nell'area adiacente determinati siti monumentali e sedi istituzionali puntualmente segnalati, producevano l'effetto esclusivo di richiamare l'attenzione dell'operatore di polizia locale addetto alla centrale operativa, al fine di favorirne un eventuale tempestivo intervento.
- Il sistema non attivava ulteriori funzionalità rispetto quelle descritte (anche eventualmente legate al comportamento dell'interessato ripreso) quali, ad esempio, la capacità di rilevare i percorsi, l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali o confronto con una campionatura precostituita.
- Il Garante, pertanto, ha ritenuto proporzionato e, quindi, ammissibile il trattamento dei dati personali che il Comune di Bergamo intendeva effettuare.

Verifica preliminare richiesta da Comune di Bergamo – 21 marzo 2013

- Il Garante, tuttavia, si è raccomandato che:
  - l'informativa, resa ai sensi dell'art. 13 del Codice, evidenziasse chiaramente che il sistema di videosorveglianza rilevava e segnalava la presenza prolungata nelle aree delimitate dalla linea di interdizione virtuale in prossimità delle sedi e degli edifici selezionati.
  - Il Comune di Bergamo ottemperasse agli obblighi relativi a:
    - le misure minime di sicurezza, con particolare riferimento all'obbligo di adottare specifici accorgimenti tecnici ed organizzativi che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa
    - i tempi di conservazione delle immagini registrate

Polizia locale: sistemi di videosorveglianza all'interno delle auto e localizzazione dei palmari posti in dotazione ai dipendenti - 8 gennaio 2015

- Con segnalazione del 22 gennaio 2014 nei confronti del Consorzio di polizia locale Valle Agno, il C.S.A. (Coordinamento Sindacale Autonomo) - Coordinamento regionale Veneto ha lamentato che all'interno delle autovetture poste in dotazione alla polizia locale sarebbe stato installato un sistema di videosorveglianza "*già in uso da due mesi*" sebbene non fosse "*stato ancora approvato un regolamento*" né alcun accordo con le rappresentanze dei lavoratori.
  - Le telecamere, fornite di "*due obiettivi che riprendono rispettivamente in orario diurno e notturno*", sarebbero state "*posizionate sul lato passeggero anteriore* [in modo da riprendere] *la parte anteriore del veicolo* [nonché] *la carreggiata ma anche il marciapiedi ai lati della stessa*".
- Il Garante ha dichiarato illeciti i trattamenti effettuati a mezzo di tali sistemi di videosorveglianza disponendo il divieto del trattamento effettuato a mezzo del sistema di localizzazione dei palmari fino all'adozione delle misure necessarie a conformare il trattamento medesimo alla disciplina in materia di protezione dei dati personali ed in materia di controllo a distanza dei dipendenti.

Quesiti

- L'ANCI ha fornito risposte ad una serie di quesiti che riguardano moltissime Amministrazioni comunali. Di seguito alcuni tra i più significativi:

  - **È necessario prevedere l'"atto di documentazione delle scelte" per l'installazione e la gestione di un sistema di videosorveglianza**?
    - NO, non è più obbligatorio, ma l'ANCI consiglia i comuni di dotarsi di un Regolamento di Gestione della videosorveglianza, affinché l'Ente individui con atto determinato le finalità e le procedure del sistema stesso.

  - **Un comune ha installato un impianto di videosorveglianza per la duplice finalità di "sicurezza urbana" e "gestione del traffico". È necessaria la verifica preliminare? E se l'impianto è collegato oltre che alla Polizia Locale, anche alle Forze di Polizia**?
    - NO, non è necessaria la verifica preliminare.

Quesiti

- **Videosorveglianza e Zone a Traffico Limitato/Corsie Bus video sorvegliate: è necessario installare l'apposita informativa, individuato nell'allegato B del Provvedimento Garante 8 aprile 2010?**
  - SI, và installato l'apposito segnale su specifica e autonoma struttura, affinché non sia visibile sul segnale stradale previsto dal Codice della Strada, ma per permettere al cittadino che accede ad una zona/area in cui sono in funzione collegate con Uffici in cu prestano servizi organi di polizia stradale

- **Le telecamere installate da un comune per finalità di "sicurezza urbana" e per la "sicurezza di edifici pubblici, sono dotate di funzione "motion detection". È necessaria la verifica preliminare?**
  - SI

Quesiti

- **Alcune pattuglie della polizia locale di un comune sono dotate di telecamere per finalità di“sicurezza urbana”, “sicurezza del personale che opera in aree a rischio” e “sanzionamento divieti di sosta – street control”. Sussiste l’obbligo di informativa e se sì come , come si adempie all’obbligo di informativa?**
  - SI, è sufficiente una indicazione segnaletica sul veicolo su cui è posizionata la telecamera mobile

- **I sistemi di videosorveglianza utilizzati per il sanzionamento degli accessi abusivi in ZTL o per il transito lungo le corsie riservate ai mezzi pubblici, che leggono le targhe dei veicoli, incrociandoli con data-base contenente le targhe autorizzate, necessitano di verifica preliminare?**
  - NO, l’associazione delle immagini non avviene con dati biometrici o sensibili e pertanto creano pregiudizio agli interessati che vengono sanzionati

Quesiti

- **Un comune ha dato in gestione e manutenzione l'impianto di videosorveglianza a una ditta privata esterna all'amministrazione comunale. Quali adempimenti devono essere osservati?**
  - La ditta deve essere nominata dal titolare dell'impianto, responsabile del trattamento e i suoi dipendenti abilitati a visionare le immagini devono ricevere una designazione ad hoc come incaricati

- **Un comune ha installato un impianto di videosorveglianza composto da una decina di telecamere e ha posizionato l'informativa indicata dal Provvedimento 8 aprile 2010, con cartelli solo all'ingresso del centro urbano. È sufficiente?**
  - NO, perché dovrebbe essere collocato prima del raggio d'azione della telecamera e se il territorio è molto vasto non avrebbe più alcun senso. Differente è l'installazione di segnali per aree, perché più circoscritte rispetto all'intero territorio comunale

Quesiti

- **Un comune ha installato un sistema di videosorveglianza per finalità di "sicurezza urbana". È vero che sono affievolite alcune prerogative e alcuni obblighi?**
  - SI (Circolare del Ministero dell'Interno del 6 agosto 2010)

- **La Questura ha chiesto ad un comune di aumentare il tempo di conservazione delle immagini, oltre i 7 giorni. Quali attività deve svolgere il comune?**
  - Il comune dovrà richiedere al Garante la "verifica preliminare", allegando la specifica richiesta della Questura e il parere del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica. Occorrerà evidenziare se l'aumento del tempo di conservazione è a carattere permanente o provvisorio.

La videosorveglianza all’interno dei luoghi di lavoro

Scuola Interregionale di Polizia Locale

Provvedimento sulla videosorveglianza: installazione nei luoghi di lavoro

- Nelle attività di sorveglianza occorre **rispettare il divieto di controllo a distanza dell'attività lavorativa**, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità.

- **Non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorati**va (ad es. orientando la telecamera sul *badge*).

- Vanno poi osservate le garanzie previste in materia di lavoro **quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro**: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, **gli impianti e le apparecchiature, "dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti***" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 D.lgs. n. 165/2001).*

Il controllo sui lavoratori

- **PRESENZA IN AZIENDA E SPOSTAMENTI PER MOTIVI DI LAVORO**
  - Controllo accessi
  - Videosorveglianza
  - Prelievo di carburante / schede
  - Antifurto satellitare
  - Navigatore satellitare
  - Telepass auto
  - RFID

Il controllo sui lavoratori

- **UTILIZZO DEL PC E DELLA RETE**
  - Dati di traffico sulla rete interna
  - Accesso alla directory ed alla posta aziendale
  - Accesso al dominio aziendale dalle postazioni
  - Log di sistema server
  - Log di sistema workstation
  - Log di dispositivi di rete
  - Log di servizi e applicazioni
  - Software installati
  - File nei serverAttachment alle e-mail
  - Proprietà e permission sui file
  - Cifratura di documenti con certificato digitale
  - Firma digitale di documenti
  - Marca temporale su documenti di proprietà
  - Share di risorse in rete
  - Indirizzo IP

Il controllo sui lavoratori

- **COMUNICAZIONI INFORMATICHE E INTERNET**
  - E-mail in entrata e in uscita su server
  - E-mail in entrata e in uscita su client
  - Log accesso internet
  - Transazioni online
  - Cache di internet
  - Cronologia navigazione
  - Sessioni di chat
  - Voice over IP
  - Fax su pc
  - Report di fax

Il controllo sui lavoratori

- **TRAFFICO TELEFONICO**
  - Tabulati telefonia fissa in entrata e in uscita
  - Dati di traffico telefonia fissa
  - Tabulati telefonia mobile

Il controllo sui lavoratori

- **ALTRI DOCUMENTI (CARTACEI E/O ELETTRONICI)**
  - Cartella del personale
  - Armadi
  - Contratti
  - Pratiche assegnate
  - Corrispondenza cartacea in entrata/uscita
  - Documenti cartacei vari
  - Registro accessi visitatori
  - Fax
  - Turni di lavoro
  - Report agenzie investigative

Il controllo sui lavoratori

ATTIVITA'

Attività preventive

- Quali informazioni **posso** raccogliere?
- Quali informazioni **devo** raccogliere?
- Per **cosa posso usare** le informazioni che vengono raccolte?
- Quali **controlli** preventivi possono essere posti in essere?
- Se dovessero servire le informazioni, come occorre acquisirle e mantenerle?

Attività reattive

- Il caso in esame quali fattispecie potrebbe configurare?
- Quali competenze occorre coinvolgere (tecniche - HR – relazioni industriali – legali)?
- Quali procedure e tempistiche prescrizionali occorre rispettare?
- Quali informazioni ci sono in azienda? Quali sono le fonti? Per quanto tempo sono conservate? Per quali motivi sono raccolte e mantenute?
- Le informazioni presenti possono essere prodotte in sede processuale?
- Le informazioni presenti potranno essere considerate dal magistrato in sede processuale a fondamento di una decisione?
- Come occorre agire per raccogliere le evidenze digitali?
    - Garanzie per il lavoratore?
    - Metodologie

I diritti e i doveri del lavoratore

- L'**articolo 2104** del **codice civile** ("***diligenza del prestatore di lavoro***") stabilisce che:
  - "*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale*.

  - *Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*".

Principali norme applicabili al controllo sui lavoratori

Statuto dei lavoratori (legge 20 maggio 1970, n. 300)

- **Articolo 1**

  I lavoratori, senza distinzione di opinioni politiche, sindacali e di fede religiosa, hanno diritto, nei luoghi dove prestano la loro opera, di manifestare liberamente il proprio pensiero, nel rispetto dei principi della Costituzione e delle norme della presente legge.

- **Articolo 2**

  Il datore di lavoro può impiegare le guardie giurate, soltanto per scopi di tutela del patrimonio aziendale.

  Le guardie giurate non possono contestare ai lavoratori azioni o fatti diversi da quelli che attengono alla tutela del patrimonio aziendale.

  Le guardie non possono accedere nei locali dove si svolge tale attività, durante lo svolgimento della stessa, se non eccezionalmente per specifiche e motivate esigenze.

Principali norme applicabili al controllo sui lavoratori

Statuto dei lavoratori (legge 20 maggio 1970, n. 300)

- **Articolo 6**

  Le visite personali di controllo sul lavoratore sono vietate fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti.

- **Articolo 7**

  Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano.

Principali norme applicabili al controllo sui lavoratori

Statuto dei lavoratori (legge 20 maggio 1970, n. 300)

- **Articolo 8**

  E' fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

Principali norme applicabili al controllo sui lavoratori

Codice penale

- **Art. 616 c.p. (Violazione, sottrazione, soppressione di corrispondenza)**

  Chiunque prende cognizione del contenuto di una corrispondenza chiusa a lui non diretta è punito…

  ➢Per "**corrispondenza**" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

Principali norme applicabili al controllo sui lavoratori

D.lgs. 196/03

- **Art. 113 (Raccolta di dati e pertinenza)**

  Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300

- **Art. 114 (Controllo a distanza)**

  Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

Il nuovo articolo 4 dello Statuto dei Lavoratori alla luce del Jobs Act e dei decreti attuativi

Articolo 4
Testo previgente

*«E' **vietato** l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da **esigenze organizzative e produttive ovvero dalla sicurezza del lavoro**, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo **accordo con le rappresentanze sindacali aziendali**, oppure, in mancanza di queste, con la **commissione interna**. In difetto di accordo, su istanza del datore di lavoro provvede la **Direzione Regionale del Lavoro** omississ»*

Le novità

ART. 23 (Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196)

1.L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente:

«ART. 4. Impianti audiovisivi e altri strumenti di controllo.

Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.

In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.

Le novità

ART. 23 (Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196)

La disposizione di cui al primo comma non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze

Le novità

ART. 23 (Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196)

Le informazioni raccolte ai sensi del primo e del secondo comma sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196».

Le novità

ART. 23 (Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196)

1. La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970

Le novità

18 giugno 2015

Controlli a distanza

•Ministero del Lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy»

•La modifica all'articolo 4 dello Statuto chiarisce, poi, che non possono essere considerati "strumenti di controllo a distanza" gli strumenti che vengono assegnati al lavoratore "per rendere la prestazione lavorativa" (una volta si sarebbero chiamati gli "attrezzi di lavoro"), come pc, tablet e cellulari.

•In tal modo, viene fugato ogni dubbio - per quanto teorico- circa la necessità del previo accordo sindacale anche per la consegna di tali strumenti.

Le novità

<u>Ministero del Lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy»</u>

•L'espressione "*per rendere la prestazione lavorativa*" comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione: ciò significa che, nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la conseguenza che queste "modifiche" possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione.

•Perciò, è bene ribadirlo, non si autorizza nessun controllo a distanza; piuttosto, si chiariscono solo le modalità per l'utilizzo degli strumenti tecnologici impiegati per la prestazione lavorativa ed i limiti di utilizzabilità dei dati raccolti con questi strumenti.

Le novità

- In definitiva:
  - Primo elemento fondamentale della proposta di riforma è che viene inserita fra le finalità perseguite la "**tutela del patrimonio aziendale**", non presente nell'attuale dizione normativa;
  - Secondo elemento fondamentale è che se chiaramente **vengono esclusi i sistemi di controllo accessi** (dovendosi intendere gli accessi fisici ai locali e, interpretando in via estensiva la parola "accesso", gli accessi logici ai sistemi informatici) **e controllo presenze** (così superando la sentenza della Corte di Cassazione n° 15892/2007), **restano in perimetro di accordo sindacale tutti i sistemi di controllo che non siano nativi dello strumento messo nella disponibilità del lavoratore o che comunque raccolgano informazioni ulteriori rispetto al mero "accesso" ai locali fisici o ai sistemi** (content filtering, data loss prevention, MAM per device mobili, geolocalizzazione)
  - Terzo elemento essenziale è che trattare legittimamente le informazioni raccolte occorre rispettare l'**obbligo informativo di cui all'art. 13 d.lgs 196/03** nonché quanto previsto dal Provvedimento dell'Autorità Garante per la protezione dei dati personali del primo marzo 2007 (adozione di un disciplinare interno redatto in forma non generica).

Il nuovo regolamento europeo

La rivoluzione privacy in Europa: cosa sta cambiando?

- **La Commissione Europea ha presentato una proposta per la tutela uniforme in materia di protezione dei dati personali:**

  - Il nuovo Regolamento UE sostituirà la direttiva 95/46/CE.

  - A differenza della direttiva, il Regolamento sarà legge direttamente applicabile in ogni Stato membro, quindi anche in Italia.

  - Il Codice Privacy ne sarà fortemente impattato.

  - La Privacy avrà regole comuni in tutti gli Stati membri

  - Alcune norme contenute nel Regolamento renderanno estremamente pesanti ed onerosi gli adempimenti per le imprese e gli enti.

La rivoluzione privacy in Europa: cosa sta cambiando?

- **Il Comitato Scientifico dell'Istituto Italiano per la Privacy, ha evidenziato gli aspetti principali caratterizzanti questa operazione normativa:**
  - allargamento dell'ambito di applicazione delle norme privacy che in un prossimo futuro potranno tutelare le informazioni dei residenti europei anche se presenti in Internet o nel cloud computing.
  - sarà imposta alle imprese l'adozione di un vero modello organizzativo per la tutela dei dati, con l'introduzione del principio di responsabilità (accountability). In concreto, saranno le aziende a dover dimostrare la conformità del loro operato alle regole comunitarie, in caso di controlli.
  - infine, colpisce l'adozione di un impianto sanzionatorio di fonte comunitaria, a garanzia dell'efficacia di quanto prescritto, con livelli massimi di rilievo, parametrati al fatturato globale annuo dell'impresa penalizzata.

La rivoluzione privacy in Europa: cosa sta cambiando?

- Gli operatori nazionali continueranno ad operare, applicando dei principi omogenei in ambito europeo. **Saranno previste più garanzie e più tutele per le persone fisiche:**

  - **Gli obiettivi infatti sono di garantire trasparenza e sicurezza**

  - **Attualmente il 72% dei cittadini europei ritieni di non aver il pieno controllo dei dati personali.**

La proposta di Regolamento UE

Articolo 22

Responsabile del Trattamento

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, il responsabile del trattamento mette in atto opportune misure ed è in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al presente regolamento.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di adeguate politiche in materia di protezione dei dati da parte del responsabile del trattamento.

L'adesione a codici di condotta approvati, ai sensi dell'articolo 38, o un meccanismo di certificazione approvato, ai sensi dell'articolo 39, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del responsabile del trattamento.

La proposta di Regolamento UE

Articolo 26

Incaricato del Trattamento

Il responsabile del trattamento ricorre unicamente a incaricati del trattamento che presentino garanzie sufficienti per mettere in atto opportune misure tecniche ed organizzative in modo tale che il trattamento soddisfi i requisiti del presente regolamento.

L'incaricato del trattamento non ricorre ad un altro incaricato senza il previo consenso specifico o generale per iscritto del responsabile del trattamento. In quest'ultimo caso l'incaricato del trattamento dovrebbe sempre informare il responsabile del trattamento di eventuali modifiche intenzionali riguardanti l'aggiunta o la sostituzione di altri incaricati del trattamento, dando così l'opportunità al responsabile del trattamento di obiettare a tali modifiche.

La proposta di Regolamento UE

Articolo 26

Incaricato del Trattamento

L'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o di uno Stato membro che vincoli l'incaricato del trattamento al responsabile del trattamento, in cui sono stipulati la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati e i diritti del responsabile del trattamento e che preveda in particolare che l'incaricato del trattamento:

a) tratti i dati personali soltanto su istruzione del responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento; in tal caso, l'incaricato del trattamento informa il responsabile del trattamento circa tale obbligo giuridico prima del trattamento dei dati, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) prenda tutte le misure richieste ai sensi dell'articolo 30;

c) rispetti le condizioni per ricorrere ad un altro incaricato del trattamento, come un requisito di autorizzazione preventiva specifica del responsabile del trattamento;

d) tenuto conto della natura del trattamento, assista il responsabile del trattamento nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

e) assista il responsabile del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 30 a 34;

f) restituisca o cancelli, a scelta del responsabile del trattamento, i dati personali al cessare della prestazione dei servizi di trattamento di dati precisati nel contratto o altro atto giuridico, salvo che il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento preveda un requisito di conservazione dei dati;

g) metta a disposizione del responsabile del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca agli audit realizzati dal responsabile del trattamento.

La proposta di Regolamento UE

Articolo 26

Incaricato del Trattamento

L'incaricato del trattamento informa immediatamente il responsabile del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o le disposizioni dell'Unione o dello Stato membro concernenti la protezione dei dati.

Fatto salvo un contratto individuale tra il responsabile del trattamento e l'incaricato del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 2 e 2 bis può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 2 ter e 2 quater o su clausole contrattuali tipo che sono parte di una certificazione concessa al responsabile del trattamento o all'incaricato del trattamento ai sensi degli articoli 39 e 39 bis.

La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 bis e in conformità della procedura d'esame di cui all'articolo 87, paragrafo 2.

Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 bis in conformità del meccanismo di coerenza di cui all'articolo 57.

Il contratto o altro atto giuridico cui si fa riferimento ai paragrafi 2 e 2 bis sono tenuti in forma scritta, anche in formato elettronico.

La proposta di Regolamento UE

Articolo 23

Protezione fin dalla progettazione e protezione di default

Tenuto conto della tecnologia disponibile e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche costituite dal trattamento, i responsabili del trattamento mettono in atto misure tecniche e organizzative adeguate all'attività di trattamento in corso e ai suoi obiettivi, quali la minimizzazione e la pseudonimizzazione dei dati, in modo tale che il trattamento soddisfi i requisiti del presente regolamento e tuteli i diritti degli interessati.

Il responsabile del trattamento mette in atto opportune misure per garantire che siano trattati, di default, solo i dati personali necessari per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e la loro accessibilità.
Quando il trattamento non è finalizzato a fornire informazioni al pubblico, detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento umano.

Un meccanismo di certificazione approvato ai sensi dell'articolo 39 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2

La proposta di Regolamento UE

Articolo 30

Misure di sicurezza

Tenuto conto della tecnologia disponibile e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento mettono in atto opportune misure tecniche e organizzative quale la pseudonimizzazione dei dati personali per garantire un livello di sicurezza adeguato al rischio.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti di dati derivanti in particolare dalla distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque elaborati.

La proposta di Regolamento UE

Articolo 30

Misure di sicurezza

L'adesione a codici di condotta approvati, ai sensi dell'articolo 38, o un meccanismo di certificazione approvato, ai sensi dell'articolo 39, può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1.

Il responsabile del trattamento e l'incaricato del trattamento fanno sì che chiunque agisca sotto l'autorità del responsabile del trattamento o dell'incaricato del trattamento e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o di uno Stato membro.

La proposta di Regolamento UE

Articolo 31

Notificazione delle violazioni di dati personali all'autorità di controllo

In caso di violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, il responsabile del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ritardo ingiustificato, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata.

La notifica prevista al paragrafo 1 non è richiesta se, ai sensi dell'articolo 32, paragrafo 3, lettere a) e b), non è richiesta una comunicazione all'interessato.

L'incaricato del trattamento informa il responsabile del trattamento senza ingiustificato ritardo dopo aver accertato la violazione dei dati personali.

La proposta di Regolamento UE

Articolo 31

Notificazione delle violazioni di dati personali all'autorità di controllo

La notifica di cui al paragrafo 1 deve come minimo:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile e appropriato, le categorie e il numero di interessati approssimativi in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione;
b) indicare l'identità e le coordinate di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le possibili conseguenze della violazione dei dati personali individuate dal responsabile del trattamento;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali; e
e) ove opportuno, indicare le misure intese ad attenuare i possibili effetti pregiudizievoli della violazione dei dati personali.

Qualora e nella misura in cui non sia possibile fornire le informazioni di cui al paragrafo 3, lettere d), e) ed f), contestualmente alle informazioni di cui ai punti a) e b), il responsabile del trattamento trasmette dette informazioni senza ulteriore ingiustificato ritardo.

Il responsabile del trattamento documenta la violazione dei dati personali di cui ai paragrafi 1 e 2, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del presente articolo.

La proposta di Regolamento UE

Articolo 32

Comunicazione delle violazioni di dati personali all'autorità di controllo

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, decifratura non autorizzata della pseudonimizzazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, il responsabile del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato di cui al paragrafo 1 descrive la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 31, paragrafo 3, lettere b), e) ed f).

Non è richiesta la comunicazione all'interessato ai sensi del paragrafo 1 se:
a. il responsabile del trattamento ha utilizzato le opportune misure tecnologiche ed organizzative di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; oppure
b. il responsabile del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c. detta comunicazione richiederebbe sforzi sproporzionati, in particolare a motivo del numero di casi in questione. In una simile circostanza, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia;
d. avrebbe ripercussioni negative su un interesse pubblico rilevante.

La proposta di Regolamento UE

Articolo 33

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, decifratura non autorizzata della pseudonimizzazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, il responsabile del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali

Il responsabile del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, chiede un parere al responsabile della protezione dei dati, qualora ne sia designato uno.

La proposta di Regolamento UE

Articolo 33

Valutazione d'impatto sulla protezione dei dati

La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei seguenti casi:
a) una valutazione sistematica e globale di aspetti della personalità degli interessati, basata sulla profilazione e da cui discendono decisioni che hanno effetti giuridici sugli interessati o incidono gravemente sugli interessati;
b) il trattamento di categorie particolari di dati personali ai sensi dell'articolo 9, paragrafo 1, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza, qualora i dati siano trattati per prendere decisioni su larga scala riguardanti persone fisiche;
c) la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi ottico-elettronici.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di operazioni di trattamento soggette al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato europeo per la protezione dei dati.

L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di operazioni di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato europeo per la protezione dei dati.

La proposta di Regolamento UE

Articolo 33

Valutazione d'impatto sulla protezione dei dati

Prima di adottare gli elenchi di cui ai paragrafi 2 bis e 2 ter, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 57 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al controllo del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

La valutazione contiene almeno una descrizione generale delle operazioni di trattamento previste, una valutazione del rischio di cui al paragrafo 1, le misure previste per affrontare il rischio, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e dei legittimi interessi degli interessati e delle altre persone in questione.

Nella valutazione della liceità e dell'impatto del trattamento compiuto dai relativi responsabili o incaricati si tiene debito conto del rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 38, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

La proposta di Regolamento UE

Articolo 33

Valutazione d'impatto sulla protezione dei dati

Il responsabile del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza delle operazioni di trattamento

Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il responsabile del trattamento è soggetto un fondamento giuridico attraverso un atto legislativo che disciplina l'operazione di trattamento specifica o l'insieme di operazioni in questione, i paragrafi 1, 2 e 3 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

La proposta di Regolamento UE

Articolo 79

Sanzioni amministrative

Ogni autorità di controllo garantisce che le **sanzioni amministrative pecuniarie** irrogate ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui all'articolo 79 bis siano in ogni singolo caso **effettive, proporzionate e dissuasive**.

Le sanzioni amministrative pecuniarie sono irrogate, in funzione delle **circostanze di ogni singolo caso**, oltre alle misure di cui all'articolo 53, paragrafo 1 ter , lettere da a) a f) o in luogo di tali misure.

Al momento di decidere se irrogare una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) **la natura, la gravità e la durata della violazione considerate la natura, la portata o la finalità del trattamento** in questione nonché il **numero di interessati lesi dal danno e il livello del danno da essi subito**;

b) il **carattere doloso o colposo** della violazione;

c) le **misure prese dal responsabile del trattamento o dall'incaricato del trattamento per attenuare il danno** subito dagli interessati;

La proposta di Regolamento UE

Articolo 79

Sanzioni amministrative

d) il **grado di responsabilità del responsabile del trattamento o dell'incaricato del trattamento** considerate le misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 23 e 30;

e) eventuali **precedenti violazioni** pertinenti commesse dal responsabile del trattamento o dall'incaricato del trattamento;

f) la **maniera in cui l'autorità di controllo ha preso conoscenza della violazione**, in particolare se e in che misura il responsabile del trattamento o l'incaricato del trattamento ha notificato la violazione;

h) qualora siano stati precedentemente imposti provvedimenti di cui all'articolo 53, paragrafo 1 ter , lettere a), d), e) e f), nei confronti del responsabile del trattamento o dell'incaricato del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

i) l'adesione ai codici di condotta approvati ai sensi dell'articolo 38 o ai meccanismi di certificazione approvati ai sensi dell'articolo 39;

j) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso.

La proposta di Regolamento UE

Articolo 79

Sanzioni amministrative

Ciascuno Stato membro può prevedere norme che dispongano se e in quale misura possano essere irrogate sanzioni amministrative pecuniarie a autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

La proposta di Regolamento UE

Articolo 79 bis

Sanzioni amministrative pecuniarie

1. L'autorità di controllo può irrogare **sanzioni amministrative pecuniarie non superiori a 250 000 EUR** o, per le imprese, **allo 0,5 % del fatturato mondiale totale annuo dell'esercizio precedente**, al responsabile del trattamento che, con dolo o colpa:

- non risponde entro il termine di cui all'articolo 12, paragrafo 2 alle richieste dell'interessato;
- fa pagare un contributo in violazione dell'articolo 12, paragrafo 4, prima frase.

La proposta di Regolamento UE

Articolo 79 bis

Sanzioni amministrative pecuniarie

2. L'autorità di controllo può irrogare **sanzioni amministrative pecuniarie non superiori a 500 000 EUR** o, per le imprese, **all'1 % del fatturato mondiale totale annuo dell'esercizio precedente**, al responsabile del trattamento o all'incaricato del trattamento che, con dolo o colpa:

•non fornisce le informazioni o fornisce informazioni incomplete o non fornisce le informazioni per tempo o in modo sufficientemente trasparente all'interessato, in violazione dell'articolo 12, paragrafo 3, e degli articoli 14 e 14 bis;
•non dà l'accesso all'interessato o non rettifica i dati personali, in violazione degli articoli 15 e 16;
•non cancella i dati personali in violazione del diritto alla cancellazione e "all'oblio" a norma dell'articolo 17, paragrafo 1, lettere a), b), d) oppure e);
•tratta dati personali in violazione del diritto di limitazione di trattamento a norma dell'articolo 17 bis oppure non informa l'interessato prima che la limitazione di trattamento sia revocata a norma dell'articolo 17 bis, paragrafo 4;

La proposta di Regolamento UE

Articolo 79 bis

Sanzioni amministrative pecuniarie

- non comunica a ciascuno dei destinatari cui il responsabile del trattamento ha trasmesso i dati personali le eventuali rettifiche, cancellazioni o limitazioni di trattamento, in violazione dell'articolo 17 ter;
- non fornisce all'interessato i dati personali che lo riguardano in violazione dell'articolo 18;
- tratta i dati personali dopo l'obiezione da parte dell'interessato a norma dell'articolo 19, paragrafo 1, e non dimostra l'esistenza di motivi legittimi preminenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- non fornisce all'interessato informazioni relative al diritto di opporsi al trattamento per finalità di marketing diretto a norma dell'articolo 19, paragrafo 2 o continua a trattare i dati per finalità di marketing diretto dopo l'obiezione da parte dell'interessato in violazione dell'articolo 19, paragrafo 2 bis;
- omette di determinare o non determina in modo sufficiente le rispettive responsabilità dei corresponsabili del trattamento, in violazione dell'articolo 24;
- omette di conservare o non conserva in modo sufficiente la documentazione di cui all'articolo 28 e all'articolo 31, paragrafo 4.

La proposta di Regolamento UE

Articolo 79 bis

Sanzioni amministrative pecuniarie

3. L'autorità di controllo può irrogare **sanzioni amministrative pecuniarie non superiori a 1 000 000 EUR** o, per le imprese, al **2 % del fatturato mondiale totale annuo dell'esercizio precedente**, al responsabile del trattamento o all'incaricato del trattamento che, con dolo o colpa:

•tratta dati personali senza una base giuridica a tal fine o non rispetta le condizioni relative al consenso, in violazione degli articoli 6, 7, 8 e 9;
•non rispetta le condizioni relative al processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione di cui all'articolo 20;
•non attua misure adeguate o non è in grado di dimostrare la conformità del trattamento, in violazione degli articoli 22 e 30;
•non designa un rappresentante, in violazione dell'articolo 25; tratta o dà istruzione di trattare dati personali in violazione dell' articolo 26;
•omette di allertare o notificare all'autorità di controllo o all'interessato una violazione di dati personali, oppure non la notifica [tempestivamente o] integralmente, in violazione degli articoli 31 e 32;

La proposta di Regolamento UE

Articolo 79 bis

Sanzioni amministrative pecuniarie

- non effettua una valutazione d'impatto sulla protezione dei dati in violazione dell'articolo 33 o tratta dati personali senza la consultazione preventiva dell'autorità di controllo, in violazione dell'articolo 34, paragrafo 2;
- fa un uso illecito di un sigillo o marchio di protezione dei dati di cui all'articolo 39 o non rispetta le condizioni e le procedure di cui agli articoli 38 bis e 39 bis;
- effettua o dà istruzione di effettuare un trasferimento di dati a un destinatario in un paese terzo o un'organizzazione internazionale in violazione degli articoli da 41 a 44;
- non si conforma a un ordine, a una limitazione provvisoria o definitiva di trattamento o a un ordine di sospensione dei flussi di dati dell'autorità di controllo, di cui all'articolo 53, paragrafo 1, o non dà l'accesso in violazione dell'articolo 53, paragrafo 2.

La proposta di Regolamento UE

Articolo 79 bis

Sanzioni amministrative pecuniarie

Se un responsabile del trattamento o un incaricato del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento elencate nei paragrafi 1, 2 o 3, l'importo totale della sanzione amministrativa pecuniaria non può superare l'importo precisato per la violazione più grave

La proposta di Regolamento UE

Articolo

Sanzioni penali

Per le violazioni del presente regolamento, in particolare per violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 79 bis, **gli Stati membri determinano le sanzioni per violazione di tali disposizioni e prendono tutti i provvedimenti necessari per la loro applicazione. Tali sanzioni sono effettive, proporzionate e dissuasive**.

Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro la data di cui all'articolo 91, paragrafo 2, **e comunica senza ritardo ogni successiva modifica**.

Gli Stati membri possono astenersi dal prevedere norme relative alle sanzioni amministrative pecuniarie a norma dell'articolo 79 bis, paragrafi 1, 2 e 3 se il loro sistema giudiziario non le prevede e le violazioni ivi enumerate sono già soggette a sanzioni penali nella loro legislazione nazionale entro [data di cui all'articolo 92, paragrafo 2], **assicurandosi nel contempo che tali sanzioni penali siano effettive, proporzionate e dissuasive in considerazione del livello di sanzioni amministrative pecuniarie previste dal presente regolamento**.
In questo caso, gli Stati membri comunicano alla Commissione le pertinenti norme di diritto penale.

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 35 **Designazione del Responsabile della protezione dei dati**	1. Il responsabile del trattamento e l'incaricato del trattamento **designano sistematicamente** un responsabile della protezione dei dati quando: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, oppure b) il trattamento è effettuato da un'impresa con 250 o più dipendenti, oppure c) le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati. 2. Nei casi di cui al paragrafo 1, lettera b), **un gruppo di imprese** può nominare **un unico responsabile** della protezione dei dati.	1. Il responsabile del trattamento **o** l'incaricato del trattamento **possono designare** o**, se previsto dal diritto dell'Unione o degli Stati membri, designano** (…) un responsabile della protezione dei dati. 2. Un **gruppo di imprese** può nominare un **unico responsabile** della protezione dei dati.

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 35 **Designazione del Responsabile della protezione dei dati**	3. Qualora il responsabile del trattamento o l'incaricato del trattamento sia un'autorità pubblica o un organismo pubblico, **il responsabile della protezione dei dati può essere designato per più enti**, tenuto conto della struttura organizzativa dell'autorità pubblica o dell'organismo pubblico. 4. Nei **casi diversi** da quelli di cui al paragrafo 1, il responsabile del trattamento, l'incaricato del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o di incaricati del trattamento **possono designare un responsabile della protezione dei dati**.	3. Qualora il responsabile del trattamento o l'incaricato del trattamento sia un'autorità pubblica o un organismo pubblico, un **unico responsabile della protezione dei dati** può essere designato per **più autorità pubbliche o organismi pubblici**, tenuto conto della loro struttura organizzativa e dimensione. 4. (…).

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 35 **Designazione del Responsabile della protezione dei dati**	5. Il responsabile del trattamento o l'incaricato del trattamento designa il responsabile della protezione dei dati **in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti di cui all'articolo 37**. Il livello necessario di conoscenza specialistica **è determinato in particolare in base al trattamento di dati effettuato e alla protezione richiesta per i dati personali trattati** dal responsabile del trattamento o dall'incaricato del trattamento.	5. Il (…) responsabile della protezione dei dati è designato **in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti di cui all'articolo 37**, in particolare **l'assenza di conflitto di interessi**. (…).

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 35 **Designazione del Responsabile della protezione dei dati**	6. Il responsabile del trattamento o l'incaricato del trattamento si assicura che ogni altra funzione professionale del responsabile della protezione dei dati **sia compatibile con i compiti e le funzioni dello stesso in qualità di responsabile della protezione dei dati e non dia adito a conflitto di interessi**. 7. Il responsabile del trattamento o l'incaricato del trattamento designa un responsabile della protezione dei dati **per un periodo di almeno due anni. Il mandato del responsabile della protezione dei dati è rinnovabile**. Durante il mandato può essere destituito solo se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni.	6. (…) 7. (…). Durante il mandato il responsabile della protezione dei dati può essere destituito, **oltre che per gravi motivi i quali, a norma del diritto dello Stato membro interessato, giustifichino la destituzione di un dipendente o di un funzionario pubblico**, solo se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni a norma dell'articolo

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 35 **Designazione del Responsabile della protezione dei dati**	8. Il responsabile della protezione dei dati può essere **assunto** dal responsabile del trattamento o dall'incaricato del trattamento **oppure adempiere ai suoi compiti in base a un contratto di servizi**. 9. Il responsabile del trattamento o l'incaricato del trattamento **comunica il nome e le coordinate di contatto del responsabile della protezione dei dati all'autorità di controllo e al pubblico**. 10. Gli interessati hanno il diritto di **contattare** il responsabile della protezione dei dati **per tutte le questioni relative al trattamento dei loro dati personali e presentare richieste per esercitare i diritti riconosciuti dal presente regolamento**.	8. Il responsabile della protezione dei dati **può essere un membro del personale** del responsabile del trattamento o dell'incaricato del trattamento oppure **adempiere ai suoi compiti in base a un contratto di servizi**. 9. Il responsabile del trattamento o l'incaricato del trattamento **pubblica le coordinate di contatto del responsabile della protezione dei dati e le comunica all'autorità di controllo (…).** 10. Gli interessati possono **contattare** il responsabile della protezione dei dati **per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti riconosciuti dal presente regolamento**.

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 35 **Designazione del Responsabile della protezione dei dati**	11. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86 al fine di **precisare i criteri e i requisiti concernenti le attività principali del responsabile del trattamento o dell'incaricato del trattamento** di cui al paragrafo 1, lettera c), e **i criteri relativi alle qualità professionali del responsabile della protezione dei dati** di cui al paragrafo 5.	11. (…)

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 36 **Posizione del responsabile della protezione dei dati**	1. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati **sia prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali**.	1. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati sia **prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.**
	2. Il responsabile del trattamento o l'incaricato del trattamento **si assicura che il responsabile della protezione dei dati adempia alle funzioni e ai compiti in piena indipendenza e non riceva alcuna istruzione per quanto riguarda il loro esercizio. Il responsabile della protezione dei dati riferisce direttamente ai superiori gerarchici del responsabile del trattamento o dell'incaricato del trattamento.**	2. Il responsabile del trattamento o l'incaricato del trattamento **sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 37 fornendogli (…) le risorse necessarie per adempiere a tali compiti nonché l'accesso ai dati personali e alle operazioni di trattamento.**

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 36 **Posizione del responsabile della protezione dei dati**	3. Il responsabile del trattamento o l'incaricato del trattamento **sostiene il responsabile della protezione dei dati nell'esecuzione dei suoi compiti e gli fornisce personale, locali, attrezzature e ogni altra risorsa necessaria per adempiere alle funzioni e ai compiti di cui all'articolo 37.**	3. Il responsabile del trattamento o l'incaricato del trattamento **si assicura che il responsabile della protezione dei dati possa agire in maniera indipendente nell'adempimento dei propri compiti e non riceva alcuna istruzione per quanto riguarda il loro esercizio**. Il responsabile della protezione dei dati **non è penalizzato dal responsabile del trattamento o dall'incaricato del trattamento per l'adempimento dei propri compiti**. **Il responsabile della protezione dei dati riferisce direttamente ai massimi superiori gerarchici del responsabile del trattamento o dell'incaricato del trattamento.** 4. Il responsabile della protezione dei dati **può svolgere altri compiti e funzioni**. Il responsabile del trattamento o l'incaricato del trattamento **si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.**

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 37 **Compiti del Responsabile della protezione dei dati**	1. Il responsabile del trattamento o l'incaricato del trattamento conferisce al responsabile della protezione dei dati almeno i seguenti compiti: a) **informare e consigliare** il responsabile del trattamento o l'incaricato del trattamento in merito **agli obblighi derivanti dal presente regolamento e conservare la documentazione relativa a tale attività e alle risposte ricevute**; b) sorvegliare l'attuazione e l'applicazione delle **politiche del responsabile del trattamento o dell'incaricato del trattamento in materia di protezione dei dati personali**, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi;	1. Il (…) responsabile della protezione dei dati è (...) incaricato delle seguenti funzioni: a) **informare e consigliare** il responsabile del trattamento o l'incaricato del trattamento **nonché i dipendenti che trattano dati personali** in merito **agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati** (…); b) sorvegliare **l'osservanza del presente regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati** nonché delle **politiche del responsabile del trattamento o dell'incaricato del trattamento in materia di protezione dei dati personali**, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e gli audit connessi;

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 37 **Compiti del Responsabile della protezione dei dati**	c) sorvegliare **l'attuazione e l'applicazione del presente regolamento, con particolare riguardo ai requisiti concernenti la protezione fin dalla progettazione, la protezione di default, la sicurezza dei dati, l'informazione dell'interessato e le richieste degli interessati di esercitare i diritti riconosciuti dal presente regolamento**;	c) (...)
	d) garantire **la conservazione della documentazione** di cui all'articolo 28;	d) (...)
	e) controllare **che le violazioni dei dati personali siano documentate, notificate e comunicate ai sensi degli articoli** 31 e 32;	e) (...)
	f) controllare **che il responsabile del trattamento o l'incaricato del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva** nei casi previsti dagli articoli 33 e 34;	f) fornire, se richiesto, **un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento** ai sensi dell'articolo 33;

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 37 **Compiti del Responsabile della protezione dei dati**	g) controllare che **sia dato seguito alle richieste dell'autorità di controllo** e, nell'ambito delle sue competenze, **cooperare con l'autorità di controllo** di propria iniziativa o su sua richiesta; h) fungere **da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento e, se del caso, **consultare l'autorità di controllo di propria iniziativa**.	g) controllare che **sia dato seguito alle richieste dell'autorità di controllo** e, nell'ambito delle sue competenze, **cooperare con l'autorità di controllo** di propria iniziativa o su sua richiesta; h) fungere **da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento di dati personali, tra cui **la consultazione preventiva** di cui all'articolo 34 e, se del caso, **effettuare consultazioni su qualunque altra questione**.

Il Data Protection Officer

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 37 **Compiti del Responsabile della protezione dei dati**	2. Alla Commissione è conferito il potere di adottare **atti delegati** conformemente all'articolo 86 al fine di precisare **i criteri e i requisiti concernenti i compiti, la certificazione, lo status, i poteri e le risorse del responsabile della protezione** dei dati di cui al paragrafo 1.	2. (...) 2 bis. Nell'eseguire i propri compiti il responsabile della protezione dei dati **considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento**.

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 **Certificazione**	1. Gli Stati membri e la Commissione **incoraggiano**, in particolare a livello europeo, **l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati garantito** dai responsabili del trattamento e dagli incaricati del trattamento. I meccanismi di certificazione della protezione dei dati **contribuiscono alla corretta applicazione del presente regolamento, in funzione delle specificità settoriali e dei diversi trattamenti**.	1. Gli Stati membri, **il comitato europeo per la protezione dei dati** e la Commissione incoraggiano, in particolare a livello unionale, **l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento delle operazioni di trattamento effettuate** dai responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle **esigenze specifiche delle micro, piccole e medie imprese.**

La Certificazione

	Testo Commissione Europea	Testo Consiglio dei Ministri
Art. 39 **Certificazione**		**1 bis.** I meccanismi, i sigilli e i marchi approvati ai sensi del paragrafo 2 bis, **oltre ad essere stabiliti affinché vengano applicati** dai responsabili del trattamento e dagli incaricati del trattamento **soggetti al presente regolamento**, possono essere stabiliti anche **al fine di dimostrare la previsione di adeguate garanzie** da parte dei responsabili del trattamento o incaricati del trattamento **non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali** alle condizioni di cui all'articolo 42, paragrafo 2, lettera e). Detti responsabili del trattamento o incaricati del trattamento assumono **l'impegno vincolante ed esecutivo, mediante strumenti contrattuali o di altro genere, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati**.

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 **Certificazione**	2. Alla **Commissione** è conferito il potere di adottare **atti delegati** conformemente all'articolo 86 **al fine di precisare i criteri e i requisiti concernenti i meccanismi di certificazione della protezione dei dati** di cui al paragrafo 1, comprese le condizioni di rilascio e ritiro e i requisiti per il riconoscimento nell'Unione e in paesi terzi.	2. La **certificazione** ai sensi del presente articolo **non riduce la responsabilità** del responsabile del trattamento o dell'incaricato del trattamento **riguardo alla conformità al presente regolamento** e **lascia impregiudicati le funzioni e i poteri dell'autorità di controllo competente** a norma dell'articolo 51 o 51 bis. 2 bis. La **certificazione** ai sensi del presente articolo è rilasciata **dagli organismi di certificazione** di cui all'articolo 39 bis o, se del caso, **da parte dell'autorità di controllo competente** in base ai **criteri** approvati **dall'autorità di controllo competente** o, ai sensi dell'articolo 57, **dal comitato europeo per la protezione dei dati**.

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 **Certificazione**	3. La Commissione può stabilire **norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere i meccanismi di certificazione e i sigilli e marchi di protezione dei dati**. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.	3. Il responsabile del trattamento o l'incaricato del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione **trasmette all'organismo di certificazione** previsto all'articolo 39 bis o, se del caso, **all'autorità di controllo competente tutte le informazioni e gli consente l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.** 4. La certificazione viene rilasciata al responsabile del trattamento o incaricato del trattamento **per un periodo massimo di 3 anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti**. Viene **revocata dagli organismi di certificazione** di cui all'articolo 39 bis o, se del caso, **dall'autorità di controllo competente**, **qualora non siano o non siano più soddisfatte i requisiti pertinenti.** 5. Il comitato europeo per la protezione dei dati **raccoglie in un registro tutti i meccanismi di certificazione e i sigilli** di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato, ad esempio tramite il portale europeo della giustizia elettronica.

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 bis **Organismo di certificazione e relativa procedura**		1. Fatti salvi le funzioni e i poteri dell'autorità di controllo competente, di cui agli articoli 52 e 53, la certificazione viene rilasciata e rinnovata **da un organismo di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati**. Ogni Stato membro stabilisce se tali organismi di certificazione siano accreditati: a) **dall'autorità di controllo competente** ai sensi dell'articolo 51 o 51 bis, e/o b) **dall'organismo nazionale di accreditamento** designato in virtù del regolamento (CE) 765/2008 del Parlamento europeo e del Consiglio che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti conformemente alla norma EN-ISO/IEC 17065/2012 **e ai requisiti aggiuntivi stabiliti dall'autorità controllo competente** ai sensi dell'articolo 51 o 51 bis.

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 bis **Organismo di certificazione e relativa procedura**		2. L'organismo di certificazione di cui al paragrafo 1 può essere accreditato a tal fine solo se: a) riguardo al contenuto della certificazione ha **dimostrato in modo convincente alla competente autorità di controllo di essere indipendente e competente**; a bis) **si è impegnato a rispettare i criteri di cui al paragrafo 2 bis dell'articolo 39** e approvati dall'autorità di controllo competente ai sensi dell'articolo 51 o 51 bis o, ai sensi dell'articolo 57, dal comitato europeo di protezione dei dati; b) ha istituito **procedure per il rilascio, il riesame periodico e il ritiro dei sigilli e dei marchi di protezione dei dati**; c) ha istituito **procedure** e strutture atte a trattare **i reclami concernenti violazioni della certificazione o il modo in cui la certificazione è stata o è attuata** dal responsabile del trattamento o dall'incaricato del trattamento ed ha gli strumenti necessari a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; d) dimostra **in modo convincente per l'autorità di controllo competente che i compiti e le funzioni da esso svolti non danno adito a conflitto di interessi**.

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 bis **Organismo di certificazione e relativa procedura**		3. L'accreditamento degli organi di certificazione di cui al paragrafo 1 **ha luogo in base ai criteri approvati dall'autorità di controllo competente** ai sensi dell'articolo 51 o 51 bis o, ai sensi dell'articolo 57, **dal comitato europeo di protezione dei dati**. In caso di accreditamento ai sensi del paragrafo 1, lettera b), tali requisiti integrano quelli previsti dal regolamento 765/2008 nonché **le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione**. 4. **L'organismo di certificazione** di cui al paragrafo 1 è **responsabile della corretta valutazione che comporta la certificazione o la revoca di quest'ultima**, fatta salva la responsabilità del responsabile del trattamento o dell'incaricato del trattamento riguardo alla conformità al presente regolamento. **L'accreditamento è rilasciato per un periodo massimo di 5 anni e può essere rinnovato alle stesse condizioni purché l'organismo soddisfi i requisiti.** 5. **L'organismo di certificazione** di cui al paragrafo 1 **trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.**

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 bis **Organismo di certificazione e relativa procedura**		6. I **requisiti** di cui al paragrafo 3 e i criteri di cui al paragrafo 2 bis dell'articolo 39 **sono resi pubblici dall'autorità di controllo in forma facilmente accessibile**. Le autorità di controllo provvedono a **trasmetterli anche al comitato europeo per la protezione dei dati**. Il **comitato europeo per la protezione dei dati raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato,** ad esempio tramite il portale europeo della giustizia elettronica. 6 bis. Fatte salve le disposizioni del capo VIII, **l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento rilasciato all'organismo di certificazione**, di cui al paragrafo 1, **se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo non sono conformi al presente regolamento**. 7. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86 **al fine di precisare i criteri e i requisiti da tenere conto per i meccanismi di certificazione della protezione dei dati** di cui al paragrafo 1 (…).

La Certificazione

	Testo Commissione Europea	**Testo Consiglio dei Ministri**
Art. 39 bis **Organismo di certificazione e relativa procedura**		7 bis. **Il comitato europeo per la protezione dei dati fornisce alla Commissione pareri sui criteri e i requisiti** di cui al paragrafo 7. 8. La **Commissione può stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere i meccanismi di certificazione e i sigilli e marchi di protezione dei dati**. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

Videosorveglianza e Cloud

Scuola Interregionale di Polizia
Locale

business international

The Executive Network

I contratti di cloud compunting

Cos'è il cloud computing

- **<u>La definizione di cloud computing data dal National Institute Standards and Technology</u>**

- "Cloud computing is a model for enabling ubiquitous, convenient, **on-demand network access** to a **shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with **minimal management effort** or service provider interaction. This cloud model is composed of **five essential characteristics, three service models, and four deployment models**".

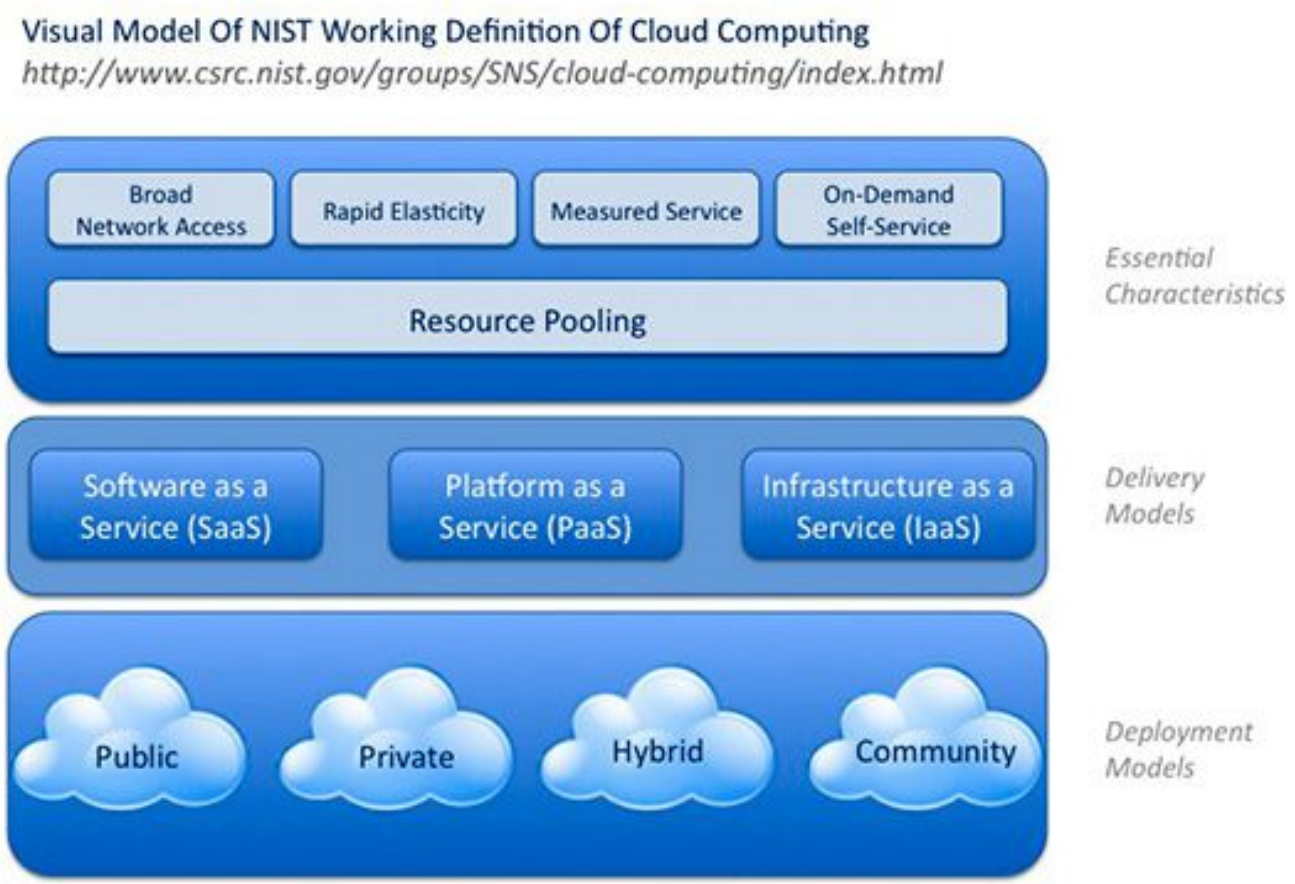
- "Il cloud computing è un modello per abilitare, **tramite la rete**, l'accesso diffuso, agevole e **a richiesta**, ad un **insieme condiviso e configurabile di risorse di elaborazione** (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con **minimo sforzo di gestione** o di interazione con il fornitore di servizi. Questo modello cloud è composto di **cinque caratteristiche essenziali, tre modalità di servizio e quattro modelli di distribuzione**".

Cos’è il cloud computing

I <u>vantaggi del cloud computing</u>

- **Accesso in mobilità** (la connessione ai dati può avvenire da qualsiasi posto e in qualsiasi momento)
- **Indipendenza dalle periferiche** (grazie alla fruizione dei servizi online, non si è vincolati ad utilizzare particolari hardware o determinate configurazioni di reti)
- **Riduzione dei costi** (acquisto, configurazione, installazione, manutenzione e dismissione di hardware e software)
- **Flessibilità e scalabilità** (è possibile agevolmente espandere o contrarre l’infrastruttura utilizzata sulla base delle contingenti o mutate esigenze aziendali)
- **Maggiore sicurezza** per la protezione dei dati.

Cos'è il cloud computing



Cos’è il cloud computing

Modelli di servizio del cloud computing		
Software as a Service (Saas)	**Platform as a Service (Paas)**	**Infrastructure as a Service (Iaas)**
Applicazione software che può essere utilizzata su richiesta. Il fornitore del servizio installa l'applicazione nei propri data center e fornisce agli utenti un’interfaccia per utilizzarla	Il fornitore mette a disposizione la propria piattaforma e offre soluzioni per lo sviluppo e l’hosting evoluto di applicazioni	Infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale è possibile installare ed eseguire il software necessario all’utente

Modelli di fruizione del cloud computing			
Private cloud	**Public cloud**	**Community cloud**	**Hybrid cloud**

Cos’è il cloud computing

- Passaggio da un modello «proprietario» di gestione delle risorse informatiche aziendali ad un modello che prevede la fruizione di un servizio.

- Importanza della disponibilità e dell’accessibilità del servizio.

- Accresciuta rilevanza del profilo contrattuale

La qualificazione giuridica dei contratti di cloud computing

- **Natura giuridica**
  - Contratto misto
  - Assenza di un profilo prevalente: nella redazione degli schemi contrattuali i fornitori oscillano tra schemi negoziali in cui prevale la struttura del contatto di appalto e schemi negoziali in cui prevale quella del contratto di licenza
  - Presenta anche una serie di affinità (e qualche differenza) rispetto ai contratti di outsourcing

La qualificazione giuridica dei contratti di cloud computing

- **Affinità rispetto al modello dell'outsourcing**

  (affidamento a terzi di determinate attività di impresa, che vengono in tal modo «esternalizzate»)

  - Esternalizzazione del servizio
  - Centralità del servizio e del suo livello qualitativo
  - Rilievo dei profili di costo ed efficienza
  - Complessità della struttura contrattuale (il contratto viene affiancato da una articolata documentazione tecnica, volta a definire gli standard della prestazione)

La qualificazione giuridica dei contratti di cloud computing

Differenze del contratto di cloud rispetto all'outsourcing

- **Prevalenza dell'organizzazione di mezzi e strutture** rispetto alla dotazione di personale
- Modello di **erogazione uno a molti**
  - **Standardizzazione** del servizio
  - **Limitata o nulla negoziabilità** delle condizioni di contratto
  - **Generale assenza di clausole di rinegoziazione** e flessibilità nell'ampiezza della durata del servizio
  - E' **il fornitore a dettare modalità di erogazione** e policies del servizio
  - **Ruolo secondario di audit e controlli diretti**
  - **Semplificazione della metrica dei costi** (frequenza di utilizzo/quantità delle risorse impiegate/durata del servizio)

La prassi contrattuale in materia di cloud computing

Marcata standardizzazione delle clausole contrattuali

- Esigenza dei cloud service provider di disciplinare e gestire in maniera uniforme una molteplicità di rapporti negoziali.
- Scarso o nullo potere negoziale degli utenti finali.

Mancanza di una specifica disciplina di legge

- Contratto atipico con causa mista.
- In mancanza di puntuale dettato contrattuale, difficoltà di inquadramento dei contratti in questione secondo le tradizionali classificazioni giuridiche (es. distinzione tra obbligazioni di mezzi ed obbligazioni di risultato).

Rigidità degli accordi , asimmetria negoziale e unfairness delle clausole

Le clausole contrattuali «critiche»

Esclusione di garanzie

•I servizi cloud sono forniti «nelle condizioni in cui si trovano» e «per quanto disponibili». In particolare, non si garantisce che i servizi offerti:

- funzionino senza interruzioni, tempestivamente, siano sicuri o privi di errori, né che eventuali errori vengano tempestivamente corretti;

- siano conformi alle specifiche esigenze dell'utente;

- non violino i diritti dei terzi (qualsiasi materiale scaricato o ottenuto dai servizi cloud, viene scaricato od ottenuto a completa discrezione ed esclusivo rischio dell'utente).

Le clausole contrattuali «critiche»

Limitazione/esclusione di responsabilità

•Escludono o limitano ad una soglia massima di danno risarcibile la responsabilità del cloud provider per danni di qualsiasi genere o natura.

•Giustificabili in ragione delle caratteristiche di multi-utenza dei contratti in questione, ma eccessivamente sbilanciate in favore del cloud provider quando ne limitino la responsabilità per danni conseguenti ad eventi che egli avrebbe l'obbligo di prevedere e gestire (es. limitazione di responsabilità in caso di perdita di dati di titolarità dell'utente).

Le clausole contrattuali «critiche»

Service Level Agreement (SLA) e meccanismi di penalizzazione

- Occorre fare attenzione:
  - Che siano fondati su parametri tecnici oggettivi e misurabili
  - Che si accompagnino alla previsione di penali, anche nella forma di service credit
  - Occorre prestare particolare attenzione alla possibilità di richiedere i danni ulteriori avendo diritti risolutori agganciati a particolari gravità di violazione o al raggiungimento di una certa entità di penali

Le clausole contrattuali «critiche»

Diritto di modifica unilaterale

• Può riguardare alternativamente o cumulativamente le condizioni tecniche e contrattuali, i livelli di servizio o i corrispettivi contrattualmente pattuiti.

• Le modifiche possono essere portate a conoscenza dell'utente tanto attraverso comunicazioni dirette, quanto attraverso mera pubblicazione sul sito web del cloud provider, imponendosi in tal modo all'utente un «onere informativo» ed un meccanismo di accettazione tacita delle condizioni modificate.

• Diritto di recesso dal contratto quale unico rimedio accordato all'utente dissenziente.

Le clausole contrattuali «critiche»

Diritto di sospensione del servizio (temporaneo o definitivo)

- Viene generalmente previsto in una o più delle seguenti ipotesi:
  - –ritardo (più o meno consistente) nel pagamento di uno o più canoni di servizio;
  - –inadempimento da parte dell'utente di una qualsiasi delle obbligazioni contrattualmente assunte;
  - –in ogni momento e per qualsiasi ragione, ad esclusiva discrezione del cloud provider.

Cloud e protezione dei dati

I principali rischi connessi all'adozione dei servizi cloud

- **Perdita del controllo** diretto ed esclusivo sui dati di propria titolarità.
- Spesso il servizio prescelto viene fornito attraverso le **prestazioni di subfornitori** diversi da quelli con cui l'utente stipula il contratto.
- La **disponibilità** dei dati allocati nella nuvola **non è incondizionatamente garantita**.
- L'utente non sempre è messo in grado di conoscere **l'ubicazione dei data center**.
- Rischio di **vendor lock-in**.
- Rischi per la **confidenzialità** e la **riservatezza** dei dati.

Cloud e protezione dei dati

Fonti normative

- Codice Privacy italiano (d. lgs. 196/2003)
- Direttiva 95/46/CE sul trattamento e la protezione dei dati personali
- Direttiva e-privacy 2002/58/CE (modificata dalla direttiva 2009/136/CE), che si applica al trattamento dei dati personali nel settore delle comunicazioni elettroniche)
- Nuovo Regolamento UE in materia di dati personali (in corso di approvazione)

Spunti di interesse provenienti da studi in ambito privacy

- Gruppo di lavoro ex art. 29, Parere 05/2012 - Cloud Computing
- La mini guida del Garante del giugno 2012 :"Proteggere i dati per non cadere dalle nuvole"
- Commission expert group

Cloud e protezione dei dati

Ripartizione di ruoli e responsabilità tra i diversi attori

Art. 4 Codice Privacy

Titolare

«La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza».

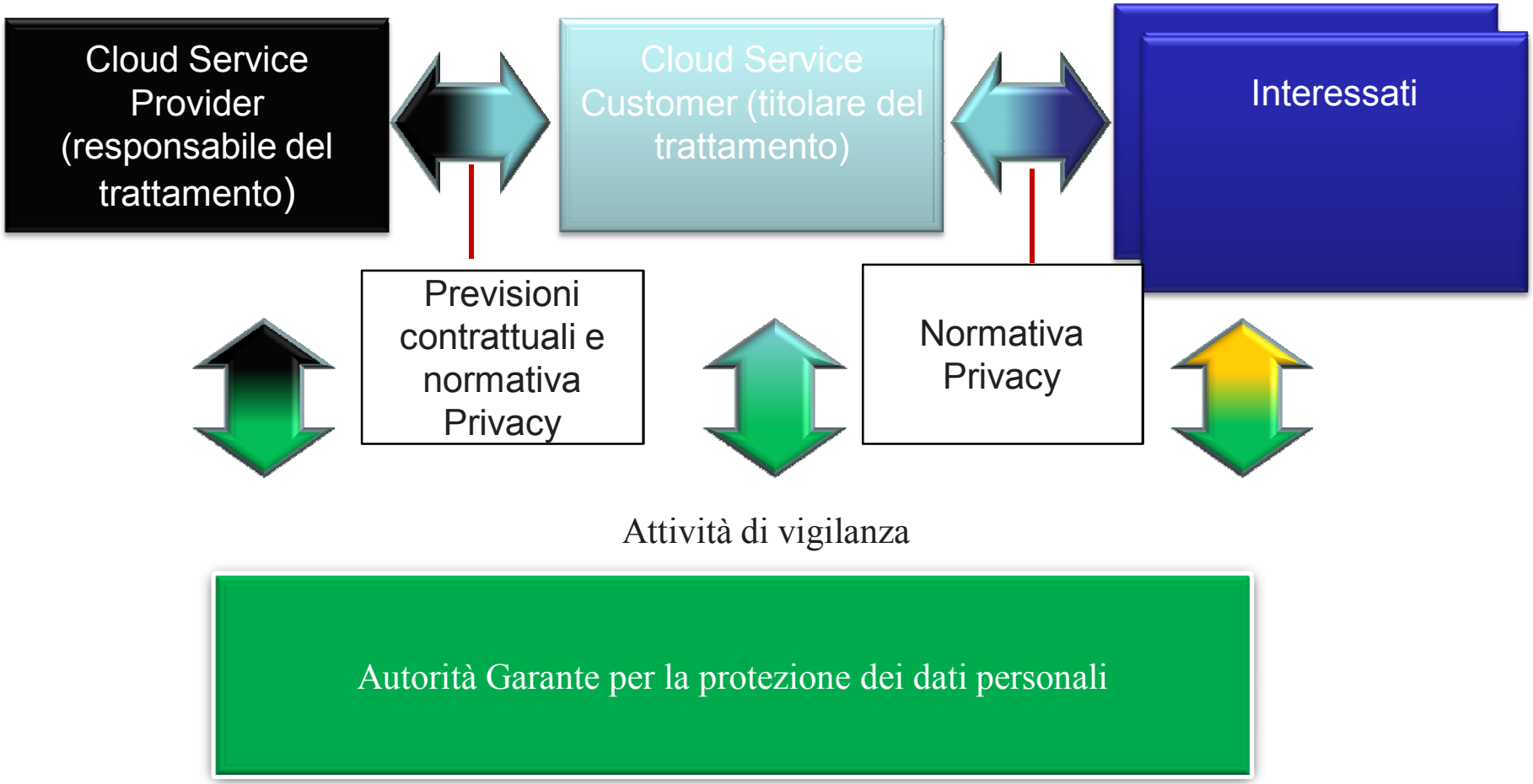
Responsabile

«La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali».

Interessato

«la persona fisica cui si riferiscono i dati personali».

Cloud e trattamento dati personali



La mini guida del Garante del giugno 2012 “Proteggere i dati per non cadere dalle nuvole”

Le indicazioni del Garante sul riparto degli obblighi tra e parti del trattamento

Un importante cambiamento per tutto il settore delle comunicazioni elettroniche, e del cloud computing in particolare, dovrebbe avvenire a breve, con l’approvazione del nuovo Regolamento generale sulla protezione dei dati (Com 2012 11 def) proposto dalla Commissione Europea. Il nuovo Regolamento introdurrà identiche regole in Europa e nei confronti di Stati terzi (riscrivendo quindi anche il Codice della privacy italiano)

Il titolare e il responsabile del trattamento.

-**La pubblica amministrazione o l’azienda, “titolare del trattamento” dei dati personali, che trasferisce del tutto o in parte il trattamento di dati personali a un fornitore, deve procedere a designare il fornitore dei servizi cloud “responsabile del trattamento”**

-**In caso di violazioni commesse dal fornitore** (o da un subfornitore), **anche il titolare sarà chiamato a rispondere dell’eventuale illecito**. Non sarà sufficiente per giustificare una eventuale violazione affermare di non avere avuto possibilità di negoziare clausole contrattuali o modalità di controllo stringenti: **il cliente di servizi cloud può sempre rivolgersi ad altri fornitori che offrono maggiori garanzie, in particolare per il rispetto della normativa sulla protezione dei dati**

-Il Codice della privacy prevede tra l’altro, che **il titolare eserciti un potere di controllo nei confronti del responsabile del trattamento**, verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati

La mini guida del Garante del giugno 2012
“Proteggere i dati per non cadere dalle nuvole”

Le indicazioni del Garante sul riparto degli obblighi tra le parti del trattamento

Trasferimento dei dati fuori dell’ Unione Europea.

-Il Codice della privacy definisce regole precise per il trasferimento dei dati personali fuori dall’ Unione europea e vieta, in linea di principio, il trasferimento “anche temporaneo” di dati personali verso uno Stato extraeuropeo, qualora l’ ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela

-**Il titolare del trattamento dovrà quindi tenere in debito conto anche il luogo dove vengono conservati i dati e quali sono i trattamenti previsti all’ estero**

Sicurezza dei dati.

-Il titolare del trattamento deve assicurarsi che siano adottate misure tecniche e organizzative volte a ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole

-**Occorre quindi contrattualmente imporre ai fornitori non solo il rispetto delle misure minime di sicurezza previste dall’ allegato B al d.lgs 196/03 ma anche un livello di sicurezza che, di volta in volta in considerazione delle caratteristiche di ogni contratto, possa essere ritenuto idoneo**

I diritti dell’ interessato.

-I soggetti pubblici e le imprese che decidono di avvalersi di servizi cloud per gestire i dati personali dei loro utenti o clienti non devono dimenticare che il Codice della privacy attribuisce agli interessati (le persone a cui si riferiscono i dati) precisi diritti

Opinion 5/2012 Art. 29 WP

I contenuti dell'opinion 5/2012 Art. 29 WP

Rapporto Titolare/Responsabile

L'Opinion 5/2012 si incentra sul paradigma cliente/fornitore = titolare/responsabile del trattamento.

Il **cliente cloud**, in qualità di **titolare del trattamento**, "*deve accettare la responsabilità dell'osservanza della legislazione sulla protezione dei dati ed è soggetto a tutti gli obblighi di legge di cui alla direttiva 95/46/CE*" ed al resto della normativa privacy (d.lgs. 196/2003 c.d. Codice Privacy, nonché la la Direttiva 2002/58/EC nel caso in cui il fornitore di servizi cloud sia anche fornitore di servizi di comunicazione elettronica accessibili al pubblico).

"*lo squilibrio fra il potere contrattuale di un piccolo responsabile del trattamento* (i.e. il titolare, per la terminologia usata dalla legislazione nazionale) *rispetto ad un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati*".

Ne consegue che il cliente cloud è tenuto a scegliere un fornitore che garantisca di fornire un servizio nel pieno rispetto della legge.

Opinion 5/2012 Art. 29 WP

I contenuti dell'opinion 5/2012 Art. 29 WP

Obblighi di protezione dei dati nella relazione cliente/fornitore

- **Trasparenza**

Deve informare tanto il rapporto tra cliente cloud ed eventuali interessati – che per legge hanno diritto a conoscere l'identità del titolare, le finalità del trattamento e i destinatario o le categorie di destinatari dei dati, che possono comprendere incaricati e subincaricati del trattamento medesimo – tanto il rapporto tra cliente cloud, cloud provider ed eventuali ulteriori subcontraenti. Sotto tale ultimo profilo, il provider sarà tenuto a fornire **un'informativa dettagliata e completa** che comprenda, tra le altre cose, **l'elenco dei responsabili e dei sub-responsabili**, **l'indicazione dei luoghi in cui i dati risiedono** o possono essere trattati, nonché precise informazioni circa la comunicazione dei dati a terzi e il trasferimento dei dati in paesi fuori dall'Unione Europea.

- **Specificazione e limitazione delle finalità del trattamento**

I dati personali dovranno essere raccolti per **finalità determinate**, **esplicite e legittime** e successivamente trattati in modo non incompatibile e non eccedente rispetto a tali finalità**.**

Opinion 5/2012 Art. 29 WP

I contenuti dell'opinion 5/2012 Art. 29 WP

Obblighi di protezione dei dati nella relazione cliente/fornitore

- **Conservazione e cancellazione dei dati**

I dati personali dovranno essere conservati in modo da consentire l'identificazione degli interessati per un arco temporale non superiore a quello strettamente necessario al conseguimento delle finalità per le quali sono rilevati o successivamente trattati. I dati personali non più necessari dovranno essere cancellati o resi anonimi. Ove la cancellazione non sia possibile stante l'esistenza di precise norme di legge che impongono la conservazione (es. normative fiscali), l'accesso a tali dati dovrà essere bloccato.

- **Tutele contrattuali nel rapporto tra Titolare e Responsabile del trattamento**

In generale: il titolare del trattamento ha l'onere di scegliere un responsabile che presenti sufficienti garanzie in termini di misure tecniche ed organizzative per la protezione e la sicurezza dei dati. Il contratto dovrà essere stipulato per iscritto e dovrà sancire in particolare l'obbligo per il responsabile di seguire le istruzioni impartite dal titolare del trattamento.

In particolare: l'opinion 5/2012 prevede una serie di contenuti contrattuali specifici che dovranno essere disciplinati al minimo negli accordi tra clienti e cloud provider.

Opinion 5/2012 Art. 29 WP

IL CONTENUTO DEI CONTRATTI
1**. Livelli di servizio** (SLA) espressi in termini **oggettivi e misurabili** e le **sanzioni correlate** al loro mancato rispetto
2. Specificazione delle **misure di sicurezza** che il fornitore cloud è tenuto a rispettare, a seconda della natura dei dati da proteggere e dei rischi del trattamento
3. **Oggetto ed orizzonte temporale** del servizio cloud da fornire
4. **Portata, modalità e finalità del trattamento dati** effettuato dal fornitore
5. Specificazione delle modalità di **restituzione** o **cancellazione dei dati** alla cessazione del rapporto
6. Previsione di una **clausola di riservatezza** vincolante per il fornitore e per i suoi dipendenti specificamente autorizzati all'accesso ai dati
7. Obbligo del fornitore di sostenere il cliente nell'agevolare l'esercizio, da parte degli interessati, dei loro **diritti di accesso ai dati, rettificazione o cancellazione**

Opinion 5/2012 Art. 29 WP

IL CONTENUTO DEI CONTRATTI
8. Obbligo del fornitore di **indicare tutti i subcontraenti autorizzati**, nonché di informare il cliente in merito ad eventuali cambiamenti degli stessi, ai quali il cliente avrà diritto di **opporsi** o di **risolvere il contratto**
9. Obbligo del fornitore di garantire che **gli accordi con i subfornitori rispecchino le disposizioni dell'accordo stipulato con il cliente**
10. Obbligo del fornitore di **comunicare al cliente eventuali violazioni** che possano costituire un rischio per i suoi dati
11. Obbligo del fornitore di **fornire un elenco dei luoghi dove saranno trattati i dati**
12. Espresso diritto del titolare di **controllare l'operato del responsabile**, a fronte del dovere di quest'ultimo di collaborare
13. Obbligo del fornitore di **informare il cliente in merito a cambiamenti rilevanti in ordine al servizio**, come l'attuazione di finalità aggiuntive

Opinion 5/2012 Art. 29 WP

IL CONTENUTO DEI CONTRATTI
14. Previsione di attività di **logging** ed **auditing** delle operazioni di trattamento dei dati personali svolte dal fornitore e dai sub contraenti
15. **Obbligo di notifica al cliente di eventuali richieste di divulgazione** di dati personali svolte da un'autorità di contrasto, salvo il caso in cui la segretezza sia prescritta per legge
16. **Garanzia di conformità alla vigente legislazione** nazionale ed internazionale dell'organizzazione interna e del sistema di trattamento utilizzato dal fornitore e dai suoi sub fornitori
17. **Diritto al risarcimento del danno** subito in conseguenza dell'illegittimo trattamento di dati personali

Opinion 5/2012 Art. 29 WP

Le misure tecniche ed organizzative
Ai sensi dell'art. 17, par. 2 Dir. 95/46/CE, il **cliente cloud**, in qualità di **titolare del trattamento**, ha la piena responsabilità della scelta di fornitori che adottino le **misure di sicurezza tecniche ed organizzative** adeguate a proteggere i dati, garantendone:
• **la disponibilità (accesso tempestivo** ed **affidabile**, prevenzione di perdita accidentale di connettività, attacchi informatici, guasti accidentali dell'hardware e altri problemi infrastrtutturali)
• **l'integrità** (in relazione all'impossibilità di **alterazione accidentale o volontaria** dei dati, durante le operazioni di trattamento, archiviazione o trasmissione)
• **l'autenticità** (mediante meccanismi di **autenticazione crittografica**, quali codici di autenticazione di messaggi o firme)

Opinion 5/2012 Art. 29 WP

Le misure tecniche ed organizzative
• **la riservatezza** (criptaggio dei dati, meccanismi di autorizzazione ed autenticazione, obblighi di riservatezza per dipendenti del fornitore e degli eventuali subfornitori)
• **l'isolamento** ("limitazione della finalità" e prevenzione del rischio di divulgazione e trattamento per scopi illegittimi)
• **la portabilità** (adozione di formati standard ed interfacce che facilitano l'interoperabilità, al fine di evitare il rischio di lock-in)

La mini guida del Garante del giugno 2012 “Proteggere i dati per non cadere dalle nuvole”

Scegliere un cloud provider di qualità: i consigli operativi del Garante
Il Garante consiglia di fare una valutazione dei rischi, costi e benefici preventiva rispetto all’utilizzo di servizi cloud.
Valutare il **tipo di cloud** e il **modello di servizio** più adatti alle proprie esigenze ed al **tipo di dati** che si ha la necessità di esternalizzare.
La voce «risparmio» non deve essere l’unico fattore di scelta.
Sfruttare l’ampiezza del mercato, scegliendo tra differenti provider.

La mini guida del Garante del giugno 2012 “Proteggere i dati per non cadere dalle nuvole”

Il decalogo del Garante
Effettuare una verifica sull’affidabilità del fornitore
Gli utenti dovrebbero accertare e valutare: **l’esperienza, la capacità e l’affidabilità del fornitore**; - la struttura societaria del fornitore, le referenze, le garanzie di legge offerte in ordine alla confidenzialità dei dati e alle misure adottate per assicurare la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti; - Gli utenti dovrebbero valutare, inoltre, le **caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità;** - Il cliente deve valutare **l’impiego da parte del fornitore di personale qualificato, l’adeguatezza delle sue infrastrutture informatiche e di comunicazione, la disponibilità ad assumersi una responsabilità risarcitoria in caso di eventuali falle nel sistema di sicurezza o di interruzioni del servizio**
Importanza delle certificazioni indipendenti (es. ISO)

La mini guida del Garante del giugno 2012 “Proteggere i dati per non cadere dalle nuvole”

Il decalogo del Garante
Privilegiare i servizi che favoriscono l’interoperabilità e la portabilità dei dati
In particolare, è consigliabile ricorrere a servizi di cloud computing privilegiando quelli basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi.
Assicurarsi la disponibilità dei dati in caso di necessità (continuità operativa e disaster recovery)
È opportuno chiedere che nel contratto con il fornitore siano ben specificate adeguate garanzie sulla disponibilità e sulle prestazioni dei servizi cloud. L’importanza degli SLA

La mini guida del Garante del giugno 2012 “Proteggere i dati per non cadere dalle nuvole”

Il decalogo del Garante
Selezionare i dati da inserire nella nuvola
Non perdere di vita di dati
È sempre opportuno che l’utente valuti accuratamente il tipo di servizio offerto, anche **verificando se i dati rimarranno nella disponibilità fisica dell’operatore con cui è stato stipulato il contratto oppure se questi svolga un ruolo di intermediario**, ovvero offra un servizio basato sulle tecnologie messe a disposizione da un operatore terzo. L’importanza della trasparenza sulla lista dei sub contractor
Informarsi su dove risiederanno concretamente i dati
È importante per l’utente sapere se i propri dati vengono trasferiti ed elaborati da server in Italia, in Europa o in un Paese extraeuropeo. Giurisdizione e legge applicabile Livello di protezione assicurato ai dati trasferiti

La mini guida del Garante del giugno 2012 “Proteggere i dati per non cadere dalle nuvole”

Il decalogo del Garante

Porre attenzione alla clausole contrattuali

È importante valutare l’idoneità delle condizioni contrattuali per l’erogazione del servizio di cloud con particolare riferimento:

- agli **obblighi e alle responsabilità in caso di perdita, distruzione o illecita diffusione dei dati** custoditi nella nuvola;
- alle modalità di esercizio del **diritto di recesso**;
- alla possibilità di **migrare ad altro fornitore;**
- alla previsione di **livelli di servizio e relative penali** per l’ipotesi di violazione;
- al **trattamento dei dati**, e specificamente:
  - **accesso ai dati** e **clausola di riservatezza;**
  - **Logging ed auditing del trattamento**;
  - **Misure tecniche ed organizzative** volte a garantire la **disponibilità, l’integrità e la riservatezza dei dati**;
- al **subappalto,** e in particolare:
  - previo consenso al subappalto da parte del titolare del trattamento;
  - obbligo di informare il titolare dell’eventuale modifica dei subappaltatori, a fronte del diritto del titolare di opporsi o risolvere il contratto;
  - responsabilità del fornitore per le violazioni poste in essere dai propri subappaltatori.

La mini guida del Garante del giugno 2012 “Proteggere i dati per non cadere dalle nuvole”

Il decalogo del Garante

Verificare il rispetto delle finalità, dei tempi e delle modalità di conservazione dei dati

In fase di acquisizione del servizio cloud è opportuno approfondire e prevedere nel contratto le politiche adottate dal fornitore riguardo a:

- tempi di conservazione dei dati;
- modalità di cancellazione.

Esigere adeguate misure di sicurezza

In generale si raccomanda di privilegiare i fornitori che utilizzino **modalità di archiviazione e trasmissione sicure, mediante tecniche crittografiche** (specialmente quando i dati trattati sono particolarmente delicati), accompagnate da **robusti meccanismi di identificazione dei soggetti autorizzati all’accesso.**

Formare adeguatamente il personale

Il personale, sia quello del cliente che quello del fornitore, incaricato del trattamento dei dati mediante servizi di cloud computing dovrebbe essere appositamente formato, al fine di limitare rischi di accesso illecito, di perdita di dati o, più in generale, di trattamento non consentito.

SAFE HARBOR ILLEGITTIMO.
QUALI SONO LE CONSEGUENZE SUI TRASFERIMENTI DEI DATI IN USA?

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

- **Trasferimento di dati all'interno dell'Unione Europea**
  - Le disposizioni del Codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

- **Trasferimento di dati al di fuori dell'Unione Europea**
  - In caso di trasferimento anche temporaneo, con qualsiasi forma o mezzo, di dati personali verso paesi non appartenenti all'Unione Europea si applicano gli articoli 43 e ss del D.lgs 196/2003.

- **La direttiva 95/46/CE si applica a tutti gli Stati membri dello Spazio Economico Europeo che comprende tutti gli Stati membri dell'Unione Europea più Norvegia, Islanda e Liechtenstein.**

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Il trasferimento dati all'estero

Il trasferimento anche temporaneo di dati personali verso un Paese terzo è, in linea di massima, **vietato**, a meno che l'ordinamento del Paese di destinazione o di transito non assicuri **un livello di tutela adeguato** (art. 25, comma 1 Direttiva 95/46 – Art. 44 D.Lgs. 196/2003).

In deroga a tale principio, **il trasferimento dei dati** verso società che hanno sede al di fuori dell'UE o del SEE **è consentito**:

•nelle **ipotesi espressamente previste** agli artt. 26, comma 1 Direttiva Privacy e 43 Codice Privacy (consenso dell'interessato e specifiche finalità del trattamento;

•quando è **autorizzato la Garante sulla base di adeguate garanzie per i diritti dell'interessato** (art. 26, comma 2 Direttiva Privacy e art. 44 Codice Privacy).

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

I trasferimenti consentiti (art. 43 D.Lgs. 196/2003)

Il **trasferimento di dati personali** verso un paese terzo **è consentito** quando:

a)l'interessato ha manifestato il proprio **consenso espresso** o, se si tratta di dati sensibili, in forma scritta;
b)è necessario per **l'esecuzione di obblighi derivanti da un contratto** del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
c)è necessario o prescritto dalla legge per la **salvaguardia di un interesse pubblico rilevante** individuato con legge o con regolamento;
d)è necessario per la **salvaguardia della vita o dell'incolumità fisica** dell'interessato o di un terzo;
e)è necessario ai fini dello **svolgimento delle investigazioni difensive** di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per **far valere o difendere un diritto in sede giudiziaria**, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
f)è effettuato in **accoglimento di una richiesta di accesso ai documenti amministrativi**, ovvero di una richiesta di **informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque**, con l'osservanza delle norme che regolano la materia;
g)è necessario per **esclusivi scopi scientifici, statistici, storici**.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

I trasferimenti consentiti (art. 43 D.Lgs. 196/2003)

Bisogna ricordare che l'Art. 29 WP ha adottato un parere nel quale afferma che **le ipotesi di esenzione** che consentono agli esportatori di trasferire dati al di fuori dell'UE senza fornire garanzie aggiuntive **si applicano solo quando i trasferimenti non sono ricorrenti, né massicci o strutturali**.

Ciò fa sì che la possibilità di applicare le deroghe previste dall'art. 43 Codice Privacy sia pressoché impossibile in relazione a ipotesi in cui in trasferimento dati sia frequente e connaturato all'oggetto del contratto (si pensi, per esempio, all'ipotesi dei servizi di coud computing).

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Altri trasferimenti consentiti (art. 44 D.Lgs. 196/2003)

Il trasferimento dei dati verso società che hanno la loro sede al di fuori della UE o del SEE è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

a)Individuate dal **Garante**:

- in relazione alle **garanzie prestate con un contratto**;
- mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo (cc.dd. **Binding Corporate Rules**).

b) Individuate dalla **Commissione Europea** mediante decisioni con cui:

- la Commissione Europea constata che un Paese non appartenente all'UE o al SEE garantisce un livello di protezione adeguato (cc.dd. **decisioni di adeguatezza)**;
- la Commissione Europea constata che alcune clausole contrattuali offrono garanzie sufficienti (cc. dd. **clausole contrattuali standard**).

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Autorizzazioni del Garante per il trasferimento dei dati sulla base delle garanzie offerte dal contratto
In questo caso il Garante deve adottare **un'autorizzazione specifica** al trasferimento
Sostanzialmente il Titolare del trattamento che intende adottare un contratto non basato su clausole contrattuali tipo deve richiedere al Garante un'autorizzazione al trasferimento dei dati verso paesi che non garantiscono un livello adeguato di protezione.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

I trasferimenti autorizzati sulla base delle decisioni di adeguatezza della Commissione Europea

La Commissione europea può stabilire, sulla base di un procedimento che prevede, fra l'altro, il **parere favorevole** del **Gruppo ex Art. 29** della **Direttiva 95/46/CE**, che il livello di protezione offerto in un determinato Paese è adeguato e che pertanto è possibile trasferirvi dati personali.

Ad oggi i Paesi che sono stati riconosciuti dalla Commissione Europea come Paesi terzi che garantiscono un livello adeguato di protezione dei dati sono: Svizzera, Andorra, Argentina, Canada, Israele, Isola di Man, Isole Fær Øer, Baliato di Jersey e Baliato di Guernsey, Nuova Zelanda, Uruguay.

Il Garante adotta di regola delle **autorizzazioni generali** al trasferimento dei dati verso i paesi che sono stati riconosciuto dalla Commissione Europea come un paese terzo che garantisce un livello adeguato di protezione dei dati.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Il Safe Harbor

Fino allo scorso 6 ottobre 2015, i trasferimenti dati verso gli **Stati Uniti** si consideravano legittimi se effettuati in conformità all'accordo del c.d. **Safe Habor** (approvato con **Decisione della Commissione Europea n. 2000/520/CE del 26 luglio 2000**).

Il programma Safe Harbor era in concreto costituito da **una serie di principi redatti dal Dipartimento del Commercio USA in accordo con la Commissione Europea**, al fine di garantire un livello adeguato di protezione dei dati personali trasferiti da persone o enti residenti in quest'ultima alle imprese aderenti aventi sede negli Stati Uniti.

I **principi del Safe Harbor non erano immediatamente precettivi per le imprese statunitensi**, ma lo diventavano una volta una volta che queste avessero aderito al programma, certificando in tal modo di **rispettare i principi contenuti nella direttiva 95/46/CE.**

Pertanto, prima di trasferire i propri dati verso una società statunitense, ogni azienda italiana aveva l'onere di verificare se la stessa fosse o meno iscritta alla Safe Harbor List.

Le imprese aderenti – il cui elenco è messo pubblicamente a disposizione dell'utenza dal Dipartimento del Commercio statunitense – sono tenute ad una "*annual reaffirmation*" dell'autocertificazione di adesione ai principi del Safe Harbor, pena la perdita dei relativi benefici.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Il Safe Harbor

Nel nostro Paese il *Safe Harbor* è stato recepito con deliberazione del Garante Privacy n. 36 del 10 ottobre 2001 "Autorizzazione al trasferimento verso gli Stati Uniti d'America".

Tuttavia, già il Gruppo di lavoro ex art 29 aveva ritenuto che **le società che esportano dati non avrebbero dovuto semplicemente basarsi sulla dichiarazione dell'importatore dei dati in merito alla certificazione Safe Harbor**.
Veniva piuttosto considerata necessaria **la prova dell'esistenza delle autocertificazioni "Safe Harbor" e, conseguentemente, richiedere che venisse dimostrata l'osservanza dei relativi principi**.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

I trasferimenti autorizzati sulla base delle clausole contrattuali tipo

Sono state individuate dalla Commissione europea delle **clausole contrattuali tipo** per il trasferimento da:

- **Titolare del trattamento a Titolare del trattamento** con le decisioni 2001/497/CE del 15 giugno 2001 e 2004/915/CE del 27 dicembre 2004
- **Titolare del trattamento a Responsabile del trattamento** con la decisione 2010/87/UE del 5 febbraio 2010

Il Titolare del trattamento che trasferisce i dati verso un paese che non garantisce un livello adeguato di protezione dei dati deve stipulare un "***data transfer agreement***" **basato sulle clausole contrattuali tipo adottate dalla Commissione Europea.**

Il Gruppo di Lavoro ex art 29 della Dir 95/46/CE ha chiarito che le clausole contrattuali possono essere **adottate soltanto per trasferimenti punto-punto** e **non possono essere utilizzate in caso di adozione di contratti multilaterali.**

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Clausole contrattuali tipo per il trasferimento da Titolare a Titolare

Sono state individuate dalla Commissione Europea delle clausole contrattuali tipo per il trasferimento da Titolare del trattamento a Titolare del trattamento con le decisioni 2001/497/CE del 15 giugno 2001 e 2004/915/CE del 27 dicembre 2004.

Il Garante in data 10 ottobre 2001 ha autorizzato i trasferimenti di dati personali dal territorio dello Stato verso paesi non appartenenti all'Unione Europea effettuati in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea 2001/497/CE.

Il Garante in data 9 giugno 2005 ha autorizzato i trasferimenti di dati personali dal territorio dello Stato verso paesi non appartenenti all'Unione Europea effettuati in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea 2004/915/CE.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Clausole contrattuali tipo per il trasferimento da Titolare a Responsabile

Sono state individuate dalla Commissione Europea delle clausole contrattuali tipo per il trasferimento da Titolare del trattamento a Responsabile del trattamento con la decisione 2010/87/UE del 5 febbraio 2010.

Il Garante in data 27 maggio 2010 ha autorizzato i trasferimenti di dati personali dal territorio dello Stato verso paesi non appartenenti all'Unione Europea effettuati in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea 2010/87/UE ciò anche con riguardo ai casi in cui **il responsabile del trattamento stabilito nell'Unione Europea, che tratta dati personali per conto di un titolare stabilito nell'Unione europea,** affidi il trattamento a un **subincaricato stabilito in un paese terzo che non assicura un livello di protezione adeguato**.

Il Garante ha altresì disposto che l'esportatore deve comunicare all'autorità l'avvenuta designazione in successione di più di un subincaricato del trattamento a seguito dell'adozione delle clausole contrattuali tipo.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Clausole contrattuali tipo per il trasferimento da Titolare a Responsabile

Il Garante in data 15 novembre 2012 ha dottato un provvedimento con il quale, fatta salva l'autonomia negoziale delle parti nella gestione dei propri rapporti commerciali ha prescritto al titolare del trattamento stabilito nel territorio dello Stato (c.d. "esportatore"), il quale abbia designato un responsabile stabilito nell'Unione europea che intenda affidare, a sua volta, il trattamento dei dati ad un altro responsabile stabilito in un Paese terzo che non assicuri un livello di protezione adeguato (c.d. "importatore"), **di conferire al responsabile con sede nella Unione europea un apposito mandato, ai sensi dell'art. 1704 c.c., per la sottoscrizione delle clausole contrattuali tipo di cui all'allegato della decisione della Commissione europea del 5 febbraio 2010, n. 87/2010/UE.** Resta comunque ferma la facoltà, per il titolare del trattamento che intenda trasferire i dati personali senza avvalersi del mandato, di chiedere al Garante **una specifica autorizzazione**.

Il Garante ha altresì disposto che il titolare del trattamento menzioni tale incarico tra i compiti attribuiti al responsabile stabilito nell'Unione europea.

Il Gruppo di Lavoro ex art 29 della Dir 95/46/CE ha proposto alla Commissione Europea una bozza di modello di clausole tipo per il trasferimento di dati tra un responsabile del trattamento stabilito nella UE e un sub-responsabile stabiliti in un Paese terzo che non assicuri un livello di protezione adeguato.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Le Clausole contrattuali tipo per il trasferimento da Titolare a Responsabile - Estratto

Clausola 4
Obblighi dell'esportatore
L'esportatore dichiara e garantisce quanto segue:
a) che **il trattamento**, compreso il trasferimento, dei dati personali, è e continua ad essere **effettuato in conformità di tutte le pertinenti disposizioni della normativa sulla protezione dei dati** (e viene comunicato, se del caso, alle competenti autorità dello Stato membro in cui è stabilito l'esportatore) nel pieno rispetto delle leggi vigenti in quello Stato;
b) che ha prescritto all'importatore, e continuerà a farlo per tutta la durata delle operazioni di trattamento, di trattare i dati personali trasferiti soltanto per suo conto e conformemente alla normativa sulla protezione dei dati e alle presenti clausole;
c) che l'importatore fornirà sufficienti garanzie per quanto riguarda le **misure tecniche e organizzative di sicurezza** indicate nell'appendice 2;
d) che, alla luce della normativa sulla protezione dei dati, le misure di sicurezza sono atte a garantire la protezione dei dati personali dalla **distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati,** segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, **o da qualsiasi altra forma illecita di trattamento di dati personali,** e che tali misure garantiscono un livello di sicurezza commisurato ai rischi inerenti al trattamento e alla natura dei dati da tutelare, tenuto conto della più recente tecnologia e dei costi di attuazione;
e) che provvederà all'osservanza delle misure di sicurezza;
f) che, qualora il trasferimento riguardi categorie particolari di dati, **gli interessati sono stati o saranno informati prima del trasferimento, o immediatamente dopo**, che i dati che li riguardano potrebbero essere trasmessi a un paese terzo che non garantisce una protezione adeguata ai sensi della direttiva 95/46/CE;
g) di trasmettere all'autorità di controllo l'eventuale comunicazione presentata dall'importatore o dal subincaricato ai sensi della clausola 5, lettera b), e della clausola 8, paragrafo 3, qualora decida di proseguire il trasferimento o revocare la sospensione;
h**) che fornirà, su richiesta degli interessati**, copia delle presenti clausole, esclusa l'appendice 2, e **una descrizione generale delle misure di sicurezza, nonché copia dei subcontratti aventi ad oggetto il trattamento da effettuarsi in conformità delle presenti clausole**, omettendo le informazioni commerciali eventualmente contenute nelle clausole o nel contratto;
i) che, in caso di subcontratto, il **subincaricato** svolge l'attività di trattamento in conformità della clausola 11 **garantendo un livello di protezione dei dati personali e dei diritti dell'interessato quanto meno uguale a quello cui è tenuto l'importatore** ai sensi delle presenti clausole;
j) che provvederà all'osservanza della clausola 4, lettere da a) ad i).

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Le Clausole contrattuali tipo per il trasferimento da Titolare a Responsabile - Estratto

Clausola 5

Obblighi dell'importatore

L'importatore dichiara e garantisce quanto segue:

a) di **trattare i dati personali esclusivamente per conto e secondo le istruzioni dell'esportatore**, nonché a norma delle presenti clausole, e di impegnarsi a informare prontamente l'esportatore qualora non possa per qualsiasi ragione ottemperare a tale disposizione, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto;

b) di non avere motivo di ritenere che la normativa ad esso applicabile impedisca di seguire le istruzioni dell'esportatore o di adempiere agli obblighi contrattuali, e di comunicare all'esportatore, non appena ne abbia conoscenza, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle presenti clausole, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto;

c) di aver applicato le **misure tecniche e organizzative di sicurezza** indicate nell'appendice 2 prima di procedere al trattamento dei dati personali trasferiti;

d) che comunicherà prontamente all'esportatore:

i) qualsiasi **richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali**, salvo che la comunicazione sia vietata da norme specifiche, ad esempio da norme di diritto penale miranti a tutelare il segreto delle indagini;

ii) qualsiasi accesso accidentale o non autorizzato; e

iii) qualsiasi richiesta ricevuta direttamente dagli interessati cui non abbia risposto, salvo che sia stato autorizzato a non rispondere;

e) che risponderà prontamente e adeguatamente a tutte le richieste dell'esportatore relative al trattamento dei dati personali soggetti a trasferimento e che si conformerà al parere dell'autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

f) **che sottoporrà i propri impianti di trattamento, su richiesta dell'esportatore, al controllo dell'esportatore o di un organismo ispettivo composto da soggetti indipendenti**, in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza e selezionati dall'esportatore, eventualmente di concerto con l'autorità di controllo;

g) che fornirà, **su richiesta degli interessati**, copia delle presenti, esclusa l'appendice 2, e **una descrizione generale delle misure di sicurezza** qualora gli interessati non siano in grado di ottenerne copia direttamente dall'esportatore, o copia dei subcontratti del trattamento, omettendo le informazioni commerciali contenute nelle clausole o nel contratto;

h) che, in caso di **subcontratto**, ha provveduto a **informare l'esportatore e ha da questi ottenuto il consenso scritto**;

i) che il subincaricato svolgerà l'attività di trattamento in conformità della clausola 11;

ii) che invierà prontamente all'esportatore copia dei subcontratti conclusi ai sensi delle presenti clausole

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Le Clausole contrattuali tipo per il trasferimento da Titolare a Responsabile - Estratto

Clausola 6

Responsabilità

1. Le parti convengono che **l'interessato che abbia subito un pregiudizio** per violazione degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera di una parte o del subincaricato **ha diritto di ottenere dall'esportatore il risarcimento del danno sofferto.**

2. Qualora l'interessato non sia in grado di proporre l'azione di risarcimento di cui al paragrafo 1 nei confronti dell'esportatore per violazione di uno degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera dell'importatore o del subincaricato, in quanto l'esportatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'importatore riconosce all'interessato stesso il diritto di agire nei suoi confronti così come se egli fosse l'esportatore, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore.

L'importatore non può far valere la violazione degli obblighi ad opera del subincaricato al fine di escludere la propria responsabilità.

3. Qualora l'interessato non sia in grado di agire in giudizio, ai fini dei paragrafi 1 e 2, nei confronti dell'esportatore o dell'importatore per violazione di uno degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera del subincaricato, in quanto sia l'esportatore che l'importatore siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, il subincaricato riconosce all'interessato stesso il diritto di agire nei suoi confronti per quanto riguarda i trattamenti da quello effettuati ai sensi delle presenti clausole così come se egli fosse l'esportatore o l'importatore, a meno che tutti gli obblighi dell'esportatore o dell'importatore siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore. La responsabilità del subincaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Le Clausole contrattuali tipo per il trasferimento da Titolare a Responsabile - Estratto

Clausola 11

Subcontratto

1. L'importatore non può subcontrattare i trattamenti effettuati per conto dell'esportatore ai sensi delle presenti clausole senza il **previo consenso scritto dell'esportatore stesso**. L'importatore che, con il consenso dell'esportatore, affidi in subcontratto l'esecuzione degli obblighi ai sensi delle presenti clausole stipula, a tal fine, con il subincaricato un accordo scritto che imponga a quest'ultimo gli obblighi cui è egli stesso tenuto in virtù delle clausole (1 **). L'importatore rimane pienamente responsabile nei confronti dell'esportatore per l'inadempimento, da parte del subincaricato, degli obblighi di protezione dei dati previsti dall'accordo scritto.**

2. Nell'accordo scritto tra l'importatore e il subincaricato è inserita la clausola del terzo beneficiario, di cui alla clausola 3, a favore dell'interessato che non sia in grado di proporre l'azione di risarcimento di cui alla clausola 6, paragrafo 1, nei confronti dell'esportatore o dell'importatore in quanto l'esportatore e l'importatore siano entrambi scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, e nessun successore abbia assunto, per contratto o per legge, l'insieme dei loro obblighi. La responsabilità civile del subincaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

3. Le disposizioni sulla protezione dei dati ai fini del subcontratto di cui al paragrafo 1 sono soggette alla legge dello Stato membro in cui è stabilito l'esportatore, ossia .....

4. **L'esportatore tiene un elenco dei subcontratti conclusi ai sensi delle presenti clausole e comunicati dall'importatore a norma della clausola 5, lettera j), e lo aggiorna almeno una volta all'anno. L'elenco sarà tenuto a disposizione dell'autorità di controllo dell'esportatore.**

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

La decisione della Corte di Giustizia dell'Unione Europea

Martedì 6 ottobre 2015, con una clamorosa sentenza resa nella causa C-362/14, **la Corte di Giustizia dell'Unione Europea** ha **dichiarato invalida la decisione n. 2000/520/CE con cui la Commissione Europea ha aderito al programma c.d. "Safe Harbor**".

Secondo quanto statuito dalla Corte di Giustizia, **i trasferimenti dati – fino a qualche giorno fa ritenuti "sicuri" – verso le aziende statunitensi che annualmente aderivano al programma "Safe Harbor" potrebbero non essere più considerati tali e, di conseguenza, essere vietati**, alla luce di quanto previsto dalla rigorosa disciplina vigente nell'Unione in materia di trasferimento di dati personali all'estero, che può aver luogo solo qualora il paese di destinazione dei dati garantisca "un livello di protezione adeguato" (art. 25, primo comma, direttiva 95/46/CE).

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

La vicenda

La vicenda da cui è scaturita la pronuncia ha avuto origine dal giudizio instaurato dal cittadino austriaco Maximillian Schrems contro l'autorità irlandese di protezione dei dati personali.

Sulla scorta delle rivelazioni rese nel 2013 da Snowden in merito alle attività dei servizi di intelligence statunitensi, **Schrems adiva l'Authority di Irlanda** (ove ha sede la filiale europea di **Facebook Inc**.), per **contestare che i propri dati**, trasferiti e trattati dall'azienda titolare dell'omonimo social network, **potessero considerarsi adeguatamente tutelati dalla sorveglianza svolta dalle autorità pubbliche degli Stati Unit**i, alla luce delle norme di diritto e delle prassi vigenti in tali Paesi.

L'Autorithy irlandese, tuttavia, respingeva la denuncia dell'attivista austriaco, nel presupposto che l'adeguatezza della protezione offerta dagli Stati Uniti ai dati personali riferiti a cittadini europei e trasferiti verso aziende aderenti al "Safe Harbor" era già stata accertata e statuita dalla Commissione Europea, con la Decisione 2000/520/CE, venendo a configurare, di fatto, un principio già "assodato".

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

La questione pregiudiziale sottoposta alla Corte

La High Court of Ireland (Alta Corte di giustizia irlandese), investita della causa, ha sollevato la questione pregiudiziale sull'interpretazione della normativa europea davanti alla Corte di Giustizia, per sapere **se la decisione della Commissione sul Safe Harbor produca l'effetto di impedire ad un'autorità nazionale di controllo di indagare su una denuncia con cui si lamenta che un paese terzo non assicura un livello di protezione adeguato** e, se necessario, di sospendere il trasferimento di dati contestato

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

La decisione della Corte

La Corte di Giustizia ha affermato che **l'esistenza di una decisione della Commissione** che dichiara che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti **non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di** controllo in forza della Carta dei diritti fondamentali dell'Unione europea e della direttiva (ivi compreso il potere di vietare un trasferimento attuato in violazione della normativa).

Questo perché:

- la Commissione non ha il potere di limitare i poteri delle autorità nazionali di controllo;
- non esiste, nell'ordinamento comunitario, alcuna disposizione che sottragga al potere di supervisione e controllo delle *Authorities* nazionali i trasferimenti verso paesi extra UE che siano stati interessati dalla cc.dd. decisioni di adeguatezza adottate dalla Commissione Europea.

Pertanto

Anche quando esiste una decisione della Commissione, le autorità nazionali di controllo, investite di una domanda, devono poter esaminare in piena indipendenza se il trasferimento dei dati di una persona verso un paese terzo rispetti i requisiti stabiliti dalla direttiva.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

La ragioni dell'invalidità del Safe Harbor

1. Nell'emanare una decisione di adeguatezza, la Commissione è chiamata a valutare se il paese destinatario del trasferimento sia in grado di offrire ai dati personali ricevuti un livello di tutela e protezione, se non identico, quantomeno "*sostanzialmente equivalente*" a quello offerto dall'ordinamento giuridico comunitario, avuto riguardo alla legislazione nazionale e agli obblighi internazionali assunti dal paese terzo. Nel caso in esame **la Commissione non ha proceduto ad una disamina del genere, ma si è limitata a valutare il Programma "Safe Harbor", il quale, peraltro, trova applicazione nei confronti delle sole aziende che annualmente decidano di aderirvi volontariamente, non vincolando in alcun modo le autorità pubbliche statunitensi**.

2. Ai sensi del quarto comma, dell'allegato I della Decisione 2000/520/CE, **l'applicabilità dei principi "Safe Harbor" può essere legittimamente limitata o sospesa** nella misura necessaria a soddisfare esigenze afferenti alla **sicurezza nazionale**, al **pubblico interesse** e **all'osservanza delle leggi statunitensi**; **cosicché le imprese americane sono tenute a disapplicare, senza limiti, le norme di tutela previste dal Safe Harbor laddove queste ultime entrino in conflitto con tali esigenze.**

3. Di fatto, **la legislazione statunitense permette alle autorità pubbliche di accedere e trattare i dati trasferiti in maniera incompatibile con la finalità per la quale è avvenuto il trasferimento**, al di là di quanto strettamente necessario e proporzionato alla tutela della sicurezza nazionale.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

L'ingerenza delle autorità pubbliche statunitensi

In sostanza, il regime americano dell'approdo sicuro rende possibili **ingerenze da parte delle autorità pubbliche americane nei diritti fondamentali delle persone**, e la decisione della Commissione non menziona l'esistenza, negli Stati Uniti, di norme intese a limitare queste eventuali ingerenze, **né l'esistenza di una tutela giuridica efficace contro tali ingerenze**.

A parere della Corte

«*una legislazione che permetta alle autorità pubbliche di avere accesso in modo generalizzato ai contenuti di comunicazioni elettroniche deve essere considerata come una compromissione dell'essenza del diritto fondamentale del rispetto della vita privata*.»

«*Allo stesso modo, una legislazione che non preveda alcuna possibilità per il singolo di esperire rimedi giuridici al fine di avere accesso ai dati personali che lo riguardano, o per ottenerne la rettifica o la cancellazione, non rispetta l'essenza del diritto fondamentale ad una tutela giurisdizionale effettiva*»

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Le conclusioni della Corte

- L'art. 25, comma sesto della direttiva 95/45/CE, letto alla luce degli artt. 7,8 e 47 della Carta dei diritti fondamentali dell'Unione Europea, deve essere interpretato nel senso che **una decisione adottata ai sensi di tale disposizione, come la decisione 2000/520/CE**, con cui la Commissione stabilisca che un paese terzo assicura un adeguato livello d protezione, **non impedisce che l'Autorità di controllo di uno Stato Mambro possa esaminare la richiesta di una persona circa la tutela dei suoi diritti,** a fronte del trasferimento dei suoi dati personali all'estero, qualora sia messo in dubbio che la legislazione e la prassi del paese terzo garantiscano un adeguato livello di protezione.

- **I poteri delle autorità nazionali di controllo sono stati limitati da una decisione della Commissione assunta in eccedenza rispetto alla proprie competenze e, pertanto, da considerarsi invalida.**

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Le conseguenza della decisione della Corte

- **La decisione 520/2000/CE con cui la Commissione ha aderito al programma Safe Harbor è invalida.**

- Venuto meno il giudizio di adeguatezza garantito dal Safe Harbor, l'ultima parola passa ai singoli Stati Membri, che potranno esercitare la propria autorità sovrana nel decidere dove vadano conservati e trattati i dati dei propri cittadini, secondo quanto stabilito all'art. 25, comma primo, dir. 95/46/CEE.

- Le autorità di controllo hanno il potere di vigilare sul rispetto delle disposizioni adottate dagli Stati membri ai sensi della direttiva nell'ambito del trasferimento di dati verso paesi terzi.

- Qualora, anche su istanza di un singolo, un'autorità di controllo ritenga che un trasferimento dati verso un paese terzo già interessato da una decisione di adeguatezza non possa considerarsi sicuro, potrà sempre adire, mediante rinvio pregiudiziale, la Corte di Giustizia, per sindacare il relativo atto di adeguatezza della Commissione europea.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Le dichiarazioni del Garante privacy italiano – 6 ottobre 2015

«Con questa sentenza la Corte di Giustizia Europea **rimette al centro dell'agenda degli Stati il tema dei diritti fondamentali delle persone e la necessità che questi diritti**, primo fra tutti la protezione dei dati, vengano tutelati anche al di fuori dei confini europei.

La Corte ha riaffermato con forza che **non è ammissibile che il diritto fondamentale alla protezione dei dati**, oggi sancito dalla Carta e dai Trattati UE, **sia compromesso dall'esistenza di forme di sorveglianza e accesso del tutto indiscriminate da parte di autorità di Paesi terz**i, che peraltro non rispettano l'ordinamento europeo sulla protezione dei dati.

E' importante peraltro sottolineare che questa sentenza, insieme ai recenti pronunciamenti della giurisprudenza europea, conferma come la Corte sempre più spesso intenda richiamare le istituzioni europee e gli Stati membri ad un rispetto reale e concreto dei principi sanciti dalla Carta dei diritti fondamentali dell'Ue.

La Corte ricorda a tutte le parti in causa che il panorama dei diritti è mutato con l'ingresso della Carta quale parte integrante dei Trattati fondamentali dell'UE, e che tutti gli strumenti e gli atti comunitari, passati e presenti, devono essere guardati con occhi nuovi, attraverso la lente della Carta.

E' la stessa ottica, del resto, in cui si muove il "pacchetto protezione dati" con il futuro Regolamento generale e la direttiva "polizia e giustizia": entrambi rafforzano, fra le altre cose, i diritti degli interessati in Ue e i poteri delle autorità nazionali di protezione dati».

«E' chiaro ora che occorre una risposta coordinata a livello europeo anche da parte dei Garanti nazionali, e in queste ore si stanno valutando le modalità più efficaci per individuare linee-guida comuni».

Il trasferimento dei dati personali all'estero:

Věra Journová – EU Commission - 6 ottobre

Věra Journová, membro della Commissione Europea, ha dichiarato che la Commissione porrà in essere una "coordinated response" tra le autorità nazionali per assicurare che vi sia un "legal framework" per le società americane.

Andrus Andrip – EU Commission - 9 ottobre 2015

Andrus Andrip, vicepresidente della Commissione, ha recentemente affermato che la Commissione intende concludere al più presto un nuovo accordo con gli USA:

«Stiamo preparando un altro accordo con gli americani
[…] Comunque lo è necessario dare in fretta una adeguata protezione ai cittadini europei».

«Ora dobbiamo lavorare insieme con gli americani per trovare una soluzione sicura»

US government (on Export.gov)

"In the current rapidly changing environment, the Department of Commerce will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework. If you have questions, please contact the European Commission, the appropriate European national data protection authority, or legal counsel".

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

The Article 29 Working Party

The Article 29 Working party, nel comunicato stampa del 6 ottobre 2015, ha affermato che il gruppo di lavoro è consapevole del fatto che questa decisione, presa nel quadro delle negoziazioni sul nuovo Regolamento europeo in materia di data protection, nonché nel contesto delle discussion tra la Commissione europea e gli USA sullo stesso Safe Harbour, ha importanti conseguenze su tutte le parti coinvolte.

Il Gruppo di lavoro ha ritenuto, quindi, di riunirsi straordinariamente, al fine di fornire un'analisi coordinata della decisione della Corte e determinare le conseguenze sui trasferimenti.

Attualmente sono in corso più serie di discussioni tra esperti.

Il trasferimento dei dati personali all'estero: cosa prevede la normativa

Gli scenari futuri

- Nuovo accordo tra USA e Europa che garatisca la legittimità dei trasferimenti dati passati e futuri (Safe Harbor 2).

- Nel frattempo, cautelativamente, le aziende che hanno sottoscritto contratti che prevedono trasferimento dati negli Stati Uniti sulla base del Safe Harbor potrebbero richiedere ai fornitori di stipulare le standard clauses della Commissione Europea per garantire la certa legittimità del trasferimento dei dati.

Grazie per l’attenzione!