Wolters Kluwer IPSOA Scuola di formazione

Il GDPR nella Pubblica

A

e soluzioni

A cura di Michele Iaselli

L’approccio del GDPR

Il Regolamento comunitario sulla protezione dei dati personali n. 2016/679 non prevede una disciplina ad hoc per il trattamento dei dati personali effettuato dai soggetti pubblici al di là di riferimenti specifici relativi all'applicazione di alcune norme o istituti, talvolta anche in regime di eccezione rispetto a regole generali.

IL GDPR, in realtà, non contiene una formale bipartizione tra titolari pubblici e privati e non contiene nemmeno norme specifiche dedicate al settore privato e pubblico, ma si occupa in generale delle condizioni di liceità del trattamento (v. art. 6 e art. 9, comma 2, per i dati particolari).

In effetti, tra gli stessi presupposti di liceità del trattamento dei dati personali il GDPR all'art. 6, lett. e) fa riferimento alla necessarietà del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, caso tipico, naturalmente dell'ente pubblico.

Si pensi, poi, all'art. 9 del GDPR che tra le eccezioni al divieto generale di trattare dati personali particolari fa rientrare:
- il trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri……;
- il trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica……;
- il trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici……;

Il d.lgs. n. 101/2018 proprio per porre rimedio all’estrema genericità della nozione di interesse pubblico contenuta nel GDPR ha individuato un elenco di trattamenti che si considerano effettuati per "motivi di interesse pubblico rilevante" (art. 2-sexies in relazione all'art. 9 del Regolamento concernente i dati che il Codice previgente definiva "dati sensibili").

Il regime normativo per tali trattamenti è sostanzialmente rimasto inalterato rispetto a quello previsto dal Codice per i trattamenti effettuati da soggetti pubblici (art. 20) e, in particolare, l'elenco predetto è tratto dalle diverse disposizioni del Codice riferite ai trattamenti effettuati per finalità di rilevante interesse pubblico (ad es. artt. 64-73, che il decreto abroga).

- accesso a documenti amministrativi e accesso civico;
- tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia;
- tenuta di registri pubblici relativi a beni immobili o mobili;
- cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- elettorato attivo e passivo ed esercizio di altri diritti politici;
- esercizio del mandato degli organi rappresentativi;
- svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo;
- attività di controllo e ispettive;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- conferimento di onorificenze e ricompense;
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- obiezione di coscienza;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario;
- istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo.

L’art. 10 del GDPR, poi, con riferimento al trattamento dei dati di rilevanza giudiziaria chiarisce che lo stesso deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Anche un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Wolters Kluwer IPSOA Scuola di formazione

La gestione dei dati personali da parte degli enti pubblici

Come è noto il Garante per la protezione dei dati personali ha suggerito più volte alle Amministrazioni pubbliche di avviare, con assoluta priorità:

- la designazione del Responsabile della protezione dei dati – RPD (artt. 37-39)
- l'istituzione del Registro delle attività di trattamento (art. 30 e cons. 171)
- la notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34)

Nell'ottica del GDPR se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

La responsabilizzazione dei titolari del trattamento dei dati è il principio fondamentale alla base del nuovo regolamento, mentre il secondo aspetto di rilievo riguarda la mappatura e la ricognizione dei trattamenti svolti dalle diverse amministrazioni e le loro principali caratteristiche".
La ricognizione sarà l'occasione per verificare il rispetto dei principi fondamentali (art. 5).

Già da questi aspetti si intuisce la necessità, anche da parte dei soggetti pubblici, di dotarsi di persone competenti nella gestione dei modelli privacy, in grado di effettuare corrette valutazioni di impatto privacy e audit pertinenti.
Da qui, si comprende la portata di un'altra disposizione di rilievo e cioè l'introduzione obbligatoria della figura del Data Protection Officer.

Wolters Kluwer IPSOA Scuola di formazione

La figura del Responsabile della Protezione dei dati (RPD | DPO)

Tra le maggiori novità del Regolamento Europeo sulla protezione dei dati personali rientra sicuramente la previsione del Data Protection Officer (DPO) o responsabile della protezione dei dati, figura di indubbio rilievo le cui competenze, per la verità, non sono state ancora chiarite nel modo migliore dagli organi comunitari.

La previsione normativa

In effetti l'art. 37 del Regolamento prevede che quando:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 (dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10
il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati (c.d. data protection officer).

Il DPO 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 propri compiti. Tale figura, di alto livello professionale, può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizi e quindi può essere un libero professionista.

Il DPO deve essere prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali sia dal titolare del trattamento che dal responsabile del trattamento e 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 derivanti dal Regolamento.

Il DPO deve godere di ampia autonomia e non riceve alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti. Inoltre il Regolamento specifica (art. 38) che il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti, ma riferisce direttamente ai massimi superiori gerarchici del titolare del trattamento o del responsabile del trattamento.

Quali sono i compiti del DPO? (art. 39 del Regolamento)

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile 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 alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nonostante tali precisazioni il DPO rimane una figura controversa che è stata molto discussa in seno alla Commissione Europea. E' sicuramente un'importante figura professionale fortemente voluta i cui compiti e responsabilità, però, non sono particolarmente chiari, specialmente avuto riferimento ai rapporti con il titolare del trattamento. E' indubbio però che il responsabile della protezione dei dati sia una figura chiave nell'ambito del trattamento automatizzato dei dati personali.

Si ricorda che in merito il WG 29 ha adottato delle Linee-guida sui responsabili della protezione dei dati (RPD) il 16 dicembre 2016 e le stesse sono state emendate in data 5 aprile 2017.

Wolters Kluwer IPSOA Scuola di formazione

Le criticità in merito al DPO nella Pubblica Amministrazione

Come noto il Regolamento n. 2016/679 chiarisce all'art. 37, par. 3 che qualora il titolare del trattamento o il responsabile 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 (ed è questo il caso presumibile dei piccoli comuni).

Per i noti problemi connessi alla scarsità di risorse della P.A. è prevedibile che la maggior parte degli enti pubblici attingeranno dal proprio personale per la designazione di un DPO e questo comporterà, indubbiamente, alcune criticità.

- Adeguata formazione del DPO
- Indipendenza del DPO
- Conflitto di interessi

Data Breach

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

L’art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata (Data breach).

Tale notifica deve come minimo:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Garante per la protezione dei dati personali già per il passato aveva adottato una serie di provvedimenti che introducevano in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali *(data breach*) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati.

- Provvedimento del Garante n. 161 del 4 aprile 2013 con il quale viene prescritto l'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) da parte dei fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali).
- Provvedimento n. 513 del 12 novembre 2014 dove viene previsto che entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

- Provvedimento n. 331 del 4 giugno 2015 dove viene sancito che entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.
- Provvedimento del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" con il quale il Garante prescrive, ai sensi dell'articolo 154, comma 1, lett. c), del Codice in materia di protezione dei dati personali, che le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare all'Autorità, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni dovevano essere redatte secondo uno schema specifico allegato al provvedimento e inviate tramite posta elettronica o posta elettronica certificata.

Proprio di recente il Garante con un Provvedimento del 30 luglio 2019 ha predisposto un modello di notifica che forma parte integrante del provvedimento ed ha sancito che i termini temporali, il contenuto e le modalità della comunicazione delle violazioni di dati personali indicati nei provvedimenti precedenti si intendono eliminati e sostituiti dai termini indicati nel GDPR e ripresi dal Provvedimento stesso.

Con quali modalità deve essere effettuata la notifica?

a) sottoscritta mediante una delle forme di cui all'articolo 20 del CAD;
b) ovvero, quando l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché attraverso uno degli altri strumenti di cui all'articolo 64, comma 2-nonies, nei limiti ivi previsti;
c) sottoscritta e presentata unitamente alla copia del documento d'identità;
c-bis) trasmessa dall'istante o dal dichiarante dal proprio domicilio digitale purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con Linee guida, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato.

L’art. 34, invece, prevede un’altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all’interessato. Difatti, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La predetta comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e non è richiesta se:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare 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 tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Procedura per la PA

Wolters Kluwer IPSOA Scuola di formazione

Registro delle attività di trattamento

L’art. 30 del Regolamento prevede che ogni titolare del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

Il registro contiene le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e di ogni contitolare del trattamento, del rappresentante del titolare del trattamento e dell'eventuale responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Anche ogni responsabile del trattamento e il suo eventuale rappresentante tengono un registro di tutte le categorie di attività di trattamento dei dati personali svolte per conto di un titolare del trattamento, contenente:

a) nome e dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e dell'eventuale responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e l'eventuale rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Registro dei trattamenti

Titolare del trattamento	Indirizzo Numero di telefono Indirizzo mail Indirizzo pec
Responsabile del Trattamento	Indirizzo Numero di telefono Indirizzo mail Indirizzo pec

Trattamento	Ufficio	Finalità	Tipi di dati personali	Categorie di interessati	Consenso	Informativa	Conservazione	Misure di sicurezza	Destinatari delle comunicazioni dei dati personali

Più nello specifico, a seguito anche di quanto consigliato dall'Autorità Garante nelle proprie FAQ datate 8 ottobre 2018, si precisa:

a) nel campo "finalità del trattamento" oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del GDPR; in merito, con particolare riferimento al "legittimo interesse", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018). Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2 del GDPR; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del GDPR;

(b) nel campo “descrizione delle categorie di interessati e delle categorie di dati personali” andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);

(c) nel campo "categorie di destinatari a cui i dati sono stati o saranno comunicati" andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;

(d) nel campo "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del GDPR (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.);

(e) nel campo "termini ultimi previsti per la cancellazione delle diverse categorie di dati" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso");

(f) nel campo "descrizione generale delle misure di sicurezza" andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del RGDP tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l'Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

Può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).

In merito, poi, al registro del responsabile del trattamento il Garante nelle proprie Faq ha precisato che:

a) nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (es. società di software house), le informazioni di cui all'art. 30, par. 2 del GDPR dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari. In questi casi il responsabile dovrà suddividere il registro in tante sezioni quanti sono i titolari per conto dei quali agisce; ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del GDPR;

b) con riferimento alla "descrizione delle categorie di trattamenti effettuati" (art. 30, par. 2, lett. b) del GDPR) è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'art. 28 del GDPR, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo;

c) in caso di sub-responsabile, parimenti, il registro delle attività di trattamento svolte da quest'ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell'art. 28, paragrafi 2 e 4 del GDPR.

L’art. 30, però, chiarisce che l’obbligo della tenuta di questi registri non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati come quelli di cui all’art. 9 del GDPR (particolari) o all’art. 10 del GDPR (dati relativi a condanne penali, reato o connessi a misure di sicurezza.

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del GDPR, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

Nella realtà, come sostenuto dai Garanti europei nelle linee guida, sono spesso i DPO a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali.

È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE.

Diventa, quindi, un'attività fondamentale dello stesso DPO per monitorare tutti i trattamenti della realtà organizzativa di riferimento.

Modalità di compilazione del registro

Lo stesso art. 30 del GDPR prevede che il registro debba rispettare la forma scritta anche in formato elettronico. In realtà l'aspetto formale poco conta (cartaceo, elettronico, struttura schematica, descrittiva, foglio di calcolo, tabella) ciò che rileva è l'esistenza di tutti gli elementi richiesti dall'art. 30 del Regolamento e l'indicazione verificabile della data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il registro dovrà recare una annotazione del tipo:

"- scheda creata in data XY"

"- ultimo aggiornamento avvenuto in data XY.

Come precisato dal Garante nelle proprie FAQ il registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile.
In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Di conseguenza, qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Le figure soggettive del mondo della protezione dei dati personali nella PA

Titolare del trattamento

Il titolare del trattamento (art. 4) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità, le condizioni e i mezzi del trattamento sono determinati dal diritto dell'Unione o dal diritto di uno Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell'Unione o dal diritto dello Stato membro.

Nell'ambito dell'organizzazione dell'ente il titolare del trattamento rimane una figura fondamentale e tale figura assume una rilevanza tale da coincidere con lo stesso concetto di titolare del trattamento di cui al nostro codice. Egli é tenuto ad adottare politiche e attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme alla normativa.

Molte di queste ultime misure sono nuove rispetto alla precedente normativa. Difatti oltre alla legittima conservazione della documentazione ed all'attuazione dei necessari requisiti di sicurezza dei dati, è prevista l'esecuzione della valutazione d'impatto sulla protezione dei dati (concetto del tutto nuovo), il rispetto dei requisiti di autorizzazione preventiva o di consultazione preventiva dell'autorità di controllo e del responsabile della protezione dei dati, la designazione di un responsabile della protezione dei dati e la definizione di informazioni e comunicazioni trasparenti da fornire all'interessato.

Il titolare del trattamento deve essere in grado di dimostrare l'efficacia di tali misure e ciò nel rispetto dell'importante principio di accountability che viene recepito dal Regolamento europeo. Per lo stesso motivo il Regolamento intende definire una responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che abbia effettuato direttamente o altri abbia effettuato per suo conto. In particolare, il titolare del trattamento deve garantire ed essere in grado di dimostrare la conformità di ogni trattamento con il Regolamento.

Altra importante novità connessa alla figura del titolare del trattamento è il recepimento dei principi della privacy by design per cui lo stesso titolare tenuto conto dell'evoluzione tecnica e dei costi di attuazione, deve mettere in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al Regolamento e assicuri la tutela dei diritti dell'interessato. In particolare, se all'interessato è lasciata facoltà di scelta relativamente al trattamento dei dati personali, il titolare del trattamento garantisce che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite.

La Realtà degli enti pubblici:

- Ministeri
- Enti locali
- Enti pubblici economici
- Agenzie

Responsabile del trattamento

Il responsabile del trattamento (art. 4) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento.
Tale figura è di tutt'altra rilevanza rispetto al passato in quanto il responsabile assume nell'ambito del Regolamento una connotazione quasi professionale.

Difatti, dice la norma (art. 28) che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato". Quindi non viene scelta una persona fisica o giuridica qualsiasi, ma chi possieda già determinate competenze, per cui appare evidente che anche il responsabile del trattamento debba avere una formazione specifica.

Inoltre il Regolamento sancisce che l'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano 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, gli obblighi e i diritti del titolare del trattamento.

Il contratto deve prevedere, in particolare, che il responsabile del trattamento:
a)tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
b)garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c)adotti tutte le misure richieste ai sensi dell'articolo 32;
d)rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e)tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f)assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36;
g)su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento
h)metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all’art. 28.

Di conseguenza lo stesso accordo tra titolare ed responsabile del trattamento deve avere un fondamento giuridico in quanto deve essere oggetto di contratto o altro atto giuridico che preveda tutta una serie di obblighi del responsabile che dipende direttamente dal titolare, può impiegare soltanto personale che si sia impegnato alla riservatezza e principalmente viene considerato anch'esso titolare del trattamento qualora tratti dati personali diversamente da quanto indicato nelle istruzioni dal titolare del trattamento.

Ciò è quanto si intuisce da quanto disciplinato dall'art. 26 del Regolamento che parla anche di contitolari del trattamento quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato.

E’ evidente, quindi, che la figura del responsabile del trattamento è connessa ad un soggetto che grazie al possesso di determinate competenze collabora concretamente con il titolare per la creazione di quelle condizioni tecniche e organizzative necessarie per l’adempimento dell’obbligo del titolare del trattamento di dare seguito alle richieste per l’esercizio dei diritti dell’interessato, assumendo peraltro determinate responsabilità derivanti dalla stipula di un accordo contrattuale.

Proprio per questi motivi lo stesso Regolamento specifica che il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.
Tra i vari obblighi, inoltre, il Regolamento pone a carico del responsabile, ma anche del titolare del trattamento l'obbligo di conservazione della documentazione di tutti i trattamenti effettuati sotto la propria responsabilità. Conservazione che se riferita a documenti informatici ovviamente implica necessarie competenze inerenti la conservazione sostitutiva.

Inoltre l'art. 28 del GDPR chiarisce che quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Non va confusa con tale figura quella prevista dall'art. 2-quaterdecies del codice in materia di protezione dei dati personali introdotto dall'art. 2 del d.lgs. n. 101/2018 che reca una serie di disposizioni volte a precisare taluni poteri e obblighi in capo al titolare e al responsabile, tra cui la possibilità di delegare compiti e funzioni a persone fisiche operanti sotto la loro autorità e responsabilità.

Tale disposizione assume una particolare rilevanza, specialmente per gli enti pubblici, proprio perché risolve in parte le diverse problematiche sorte a seguito di quanto stabilito dall'art. 28 del GDPR che concepisce il solo responsabile esterno del trattamento.
Viene poi precisato che ogni qualvolta il titolare intende effettuare un trattamento connesso all'esecuzione di un compito di pubblico interesse che presenta rischi particolarmente elevati, deve obbligatoriamente chiedere la previa autorizzazione del Garante (cfr. art. 36, comma 5, Reg).

Incaricato al trattamento

Nulla dice il Regolamento in merito alla figura dell'incaricato così come la conosciamo nel nostro Codice per la protezione dei dati personali e l'arcano è presto chiarito. Difatti la figura dell'incaricato scompare a seguito della traduzione-interpretazione in lingua italiana proposta dalla nostra Autorità Garante alla Commissione Europea ed accettata da quest'ultima. Difatti secondo l'ormai superata Direttiva 95/46/CE il "controller" era il nostro "responsabile de trattamento", mentre il "processor" era il nostro "incaricato". A seguito, invece, della proposta del Garante, alla luce dell'attuale Regolamento, per "controller" bisogna intendere "titolare del trattamento", mentre per "processor" bisogna intendere "responsabile del trattamento".

Comunque è pacifico che a prescindere da aspetti di carattere terminologico l'incaricato debba necessariamente continuare ad esistere, anche se sarebbe preferibile chiamarlo in modo diverso, ad esempio autorizzato al trattamento.

Rapporti fra privacy e trasparenza

Parlando di attività degli enti pubblici è opportuno affrontare in tale sede la delicata problematica rappresentata dal possibile conflitto tra due interessi di rango primario che, in quanto tali, devono ritenersi entrambi meritevoli di costante ed adeguata tutela da parte dell'ordinamento giuridico: quello all'informazione, che si realizza attraverso l'esercizio del diritto di accesso alla documentazione amministrativa e riposa sull'esigenza di trasparenza ed imparzialità dell'azione amministrativa; e quello alla riservatezza dei soggetti terzi, che inerisce alla sfera degli assetti privatistici e si traduce, in ultima analisi, nella necessità di garantire la segretezza dei c.d. dati sensibili, quali risultano individuati e definiti dal legislatore nella normativa di riferimento, che specificamente contiene la disciplina della protezione dei dati personali.

La giurisprudenza amministrativa ha elaborato un indirizzo interpretativo che privilegia il diritto di accesso, considerando per converso recessivo l'interesse alla riservatezza dei terzi, quando l'accesso stesso sia esercitato per la difesa di un interesse giuridico, nei limiti in cui esso sia necessario alla difesa di quell'interesse (cfr. Cons. Stato, Sez. VI, 20 aprile 2006, n. 2223).

Ma nella Pubblica Amministrazione l'atteggiamento rispetto al trattamento dei dati e delle banche dati è molto cambiato negli ultimi 20 anni, da mero adempimento si è passati ad una dimensione molto più proattiva, perché i dati e talora anche i dati personali escono sempre di più dagli uffici attraverso processi legislativi che tengono conto del loro valore economico. La PA, che fino a qualche tempo fa, gestiva passivamente i dati, oggi vuole renderli sempre più disponibili e trasparenti.

Ciò determina spesso inevitabili conflitti fra privacy e trasparenza specialmente alla luce di quanto prescritto dal d.lgs. n. 33/2013 che nel disciplinare il riutilizzo dei dati pubblicati regola necessariamente i rapporti con la normativa in materia di protezione dei dati personali chiarendo che gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari, comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali.

L’art. 7-bis del d.lgs n. 33/2013 nel disciplinare il riutilizzo dei dati pubblicati regola necessariamente i rapporti con la normativa in materia di protezione dei dati personali chiarendo che gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari, di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali.

Si precisa, inoltre, che la pubblicazione nei siti istituzionali di dati relativi a titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali sebbene la Corte Costituzionale con sentenza 23 gennaio - 21 febbraio 2019, n. 20 abbia dichiarato l'illegittimità costituzionale della disposizione dell'art. 14, comma 1-bis, del d.lgs. n. 14 marzo 2013, n. 33 nella parte in cui prevede che le pubbliche amministrazioni pubblicano i dati di cui all'art. 14, comma 1, lettera f), dello stesso decreto legislativo anche per tutti i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti, ivi inclusi quelli conferiti discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione.

La norma ancora prevede che nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

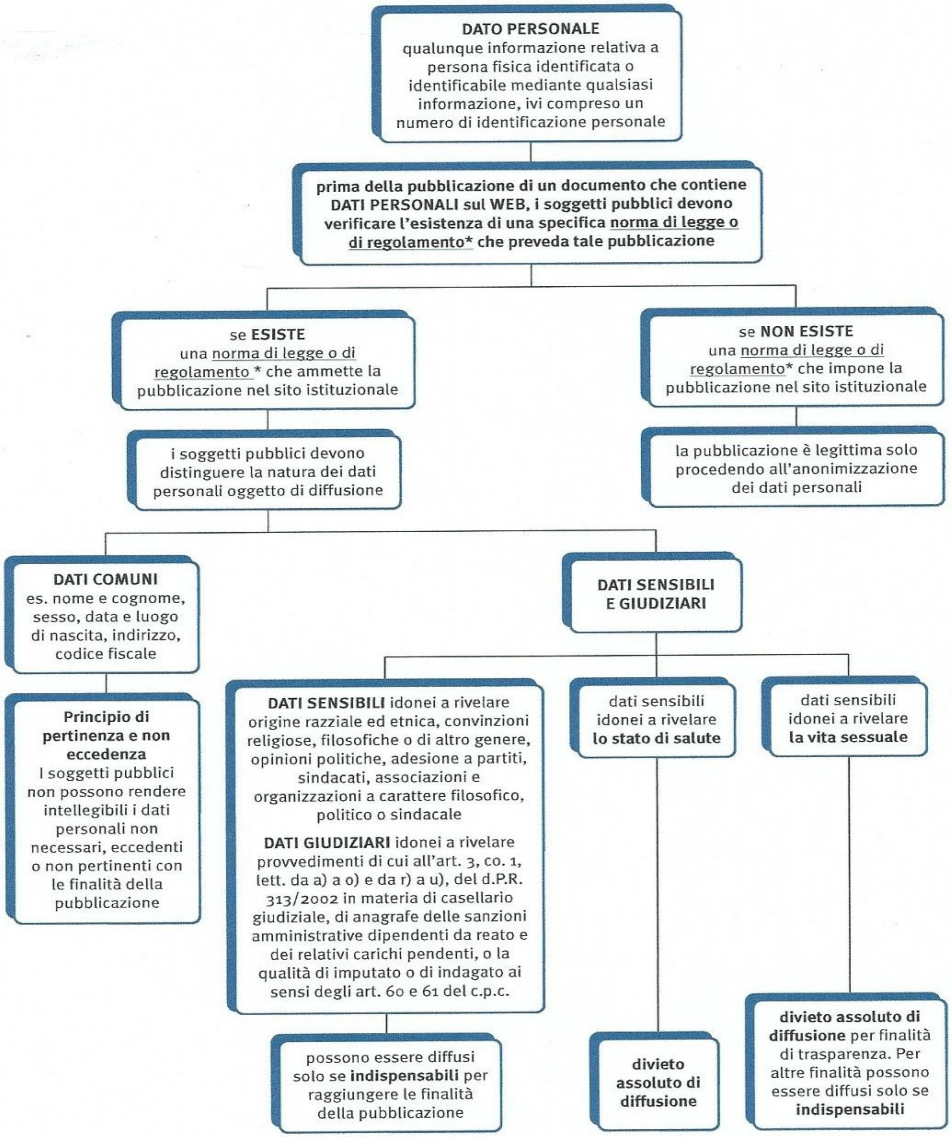
Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione sono rese accessibili dall'amministrazione di appartenenza.
Non sono invece ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione dal lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il predetto dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di carattere personale.

Sono inevitabili, quindi, in materia gli impatti con la normativa posta a tutela dei dati personali e la stessa Autorità Garante ha più volte specificato che se priva di adeguati criteri discretivi, la divulgazione di un patrimonio informativo immenso e sempre crescente (quale quello delle pubbliche amministrazioni) rischia di mettere in piazza spaccati di vita individuale la cui conoscenza è inutile ai fini del controllo sull'esercizio del potere ma, per l'interessato, può essere estremamente dannosa.

Con l'adozione di apposite Linee guida (provvedimento del 15 maggio 2014), il Garante è intervenuto proprio per assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul web di atti e documenti.
Le linee guida hanno lo scopo di individuare le cautele che i soggetti pubblici sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa.

Prima di procedere alla pubblicazione sul proprio sito web la P.A. deve:

- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;
- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;
- sottrarre all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari, come ricordato al punto precedente.


DATO PERSONALE
qualunque informazione relativa a persona fisica identificata o identificabile mediante qualsiasi informazione, ivi compreso un numero di identificazione personale
prima della pubblicazione di un documento che contiene DATI PERSONALI sul WEB, i soggetti pubblici devono verificare l'esistenza di una specifica norma di legge o di regolamento* che preveda tale pubblicazione
se ESISTE una norma di legge o di regolamento * che ammette la pubblicazione nel sito istituzionale
se NON ESISTE una norma di legge o di regolamento* che impone la pubblicazione nel sito istituzionale
i soggetti pubblici devono distinguere la natura dei dati personali oggetto di diffusione
la pubblicazione è legittima solo procedendo all'anonimizzazione dei dati personali
DATI COMUNI
es. nome e cognome, sesso, data e luogo di nascita, indirizzo, codice fiscale
DATI SENSIBILI E GIUDIZIARI
Principio di pertinenza e non eccedenza
I soggetti pubblici non possono rendere intellegibili i dati personali non necessari, eccedenti o non pertinenti con le finalità della pubblicazione
DATI SENSIBILI idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale
DATI GIUDIZIARI idonei a rivelare provvedimenti di cui all'art. 3, co. 1, lett. da a) a o) e da r) a u), del d.P.R. 313/2002 in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli art. 60 e 61 del c.p.c.
dati sensibili idonei a rivelare lo stato di salute
dati sensibili idonei a rivelare la vita sessuale
possono essere diffusi solo se indispensabili per raggiungere le finalità della pubblicazione
divieto assoluto di diffusione
divieto assoluto di diffusione per finalità di trasparenza. Per altre finalità possono essere diffusi solo se indispensabili

Un eccesso indiscriminato di pubblicità rischia, peraltro, di occultare informazioni realmente significative con altre del tutto inutili, così ostacolando, anziché agevolare, il controllo diffuso sull'esercizio del potere e degenerando in una forma di sorveglianza massiva.

Per la trasparenza c'è bisogno di un approccio qualitativo e non meramente quantitativo: meno dati ma più qualificati.

Critica è la posizione dell'Autorità garante anche con riferimento all'accesso universale ritenuto troppo ampio in quanto non prevede quelle cautele dettate dalla l. 241/1990 per l'accesso ad atti amministrativi contenenti dati sensibili o giudiziari e, soprattutto, la regola del "pari rango" per i dati ipersensibili, secondo cui ove siano coinvolti dati sanitari o sulla vita sessuale, l'accesso è ammesso solo per la tutela di una situazione giuridicamente rilevante di rango "almeno pari" o di un "altro" diritto o libertà fondamentale e inviolabile.

Secondo l'Autorità, quindi, l'attuale disciplina sulla trasparenza andrebbe rimodulata, prevedendo che ove l'accesso coinvolga dati personali di terzi, esso possa essere effettuato solo previo accertamento della prevalenza dell'interesse perseguito dall'accesso ovvero, previo oscuramento dei dati personali presenti.

Tale previsione andrebbe poi completata con un generale divieto di comunicazione di dati sensibili o giudiziari nonché di dati personali di minorenni, in osservanza della tutela rafforzata accordata dall'ordinamento interno e dal diritto dell'Unione europea a tali categorie di dati personali.

Wolters Kluwer IPSOA Scuola di formazione

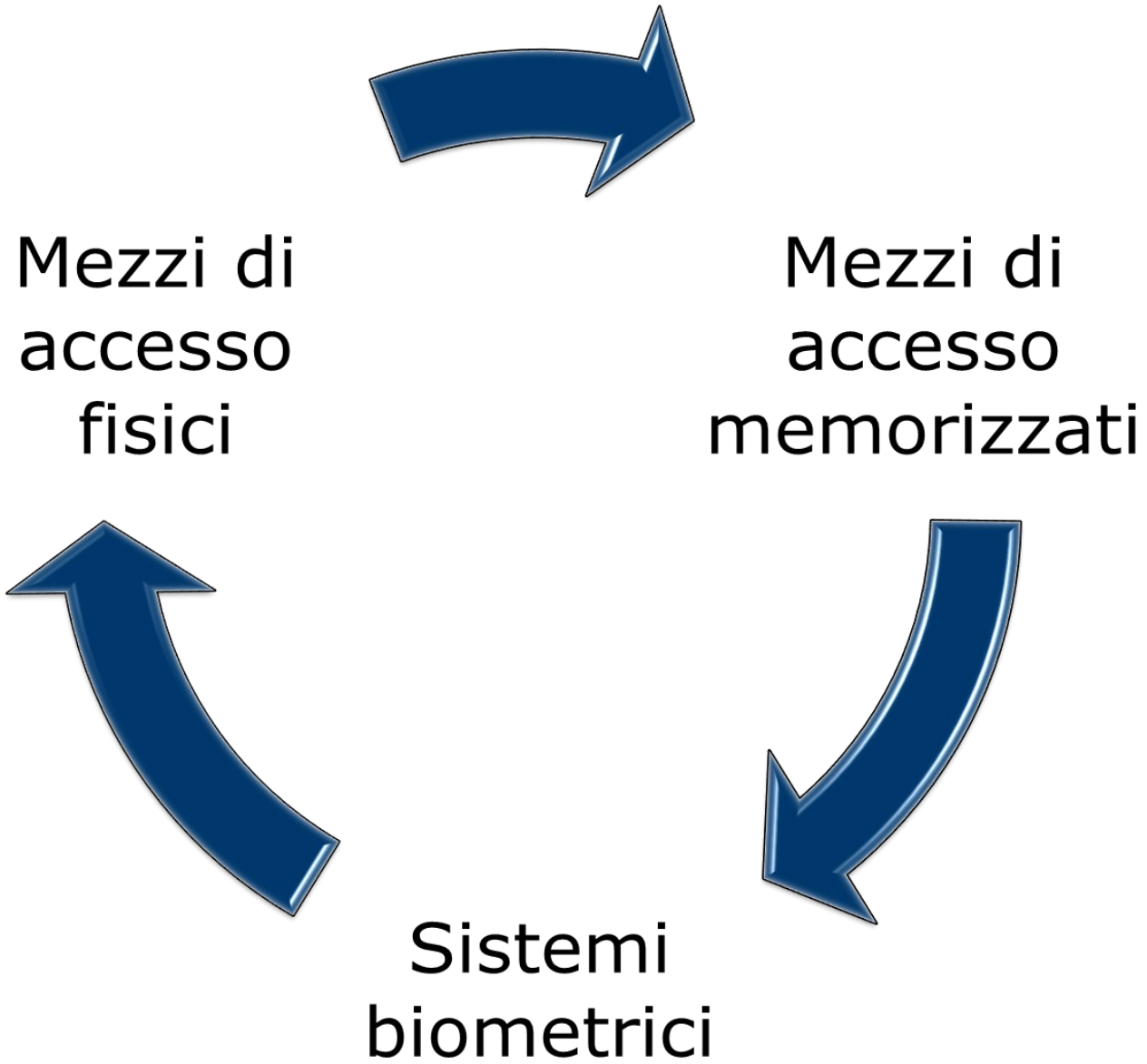
La sicurezza dei dati nella PA

La sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.
Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i data base, la trasmissione dati e la elaborazione a distanza (informatica distribuita).

Riguardo l'aspetto "sicurezza" connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati.

Come può essere garantita la sicurezza?


Mezzi di accesso fisici
Mezzi di accesso memorizzati
Sistemi biometrici

Il tema della sicurezza dei dati nella PA specialmente con l'avvento dell'informatica riveste un'importanza fondamentale perché necessaria per garantire la disponibilità, l'integrità e la riservatezza delle informazioni del Sistema informativo della Pubblica amministrazione.

Negli ultimi anni il numero complessivo di attacchi e di incidenti legati alla sicurezza informatica nella PA è aumentato in modo esponenziale. Tutti gli studi e le ricerche che analizzano e studiano questi fenomeni sono concordi nell'affermare una preoccupante tendenza alla crescita.

Le pubbliche amministrazioni, dal punto di vista sicurezza, possono essere considerate come organizzazioni fortemente regolate, in considerazione del fatto che la loro attività si svolge nell'ambito e nei limiti di norme che hanno valore di legge. Il problema è che fino ad oggi sono state poche le norme giuridiche che si siano occupate di cyber security.

In particolare negli articoli 50 e 51 del CAD si parla rispettivamente di disponibilità ed accessibilità dei dati al di fuori dei limiti di carattere normativo come nel caso della protezione dei dati personali, di sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni, regolamentati dalle misure minime di sicurezza previste dalla normativa sulla protezione dei dati personali.

In materia, difatti, occorrono ulteriori regole tecniche che in coerenza con la disciplina in materia di tutela della privacy introducano elementi utili per riconoscere l'esattezza, la disponibilità, l'integrità e per verificare l'accessibilità e la riservatezza dei dati.

Proprio per questi motivi è stata pubblicata sulla G.U. (Serie Generale n. 79 del 04/04/2017) la Circolare AgID del 17 marzo 2017 n. 1/2017 contenente le "Misure minime di sicurezza ICT per le pubbliche amministrazioni"successivamente sostituita dalla circolare n. 2/2017 del 18 aprile 2017.

Le stesse misure sono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione, emesso come previsto dal Piano Triennale per l'Informatica nella PA e dalla Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri, che assegna all'Agenzia per l'Italia Digitale il compito di sviluppare gli standard di riferimento per le amministrazioni.

Tale Direttiva in considerazione dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, sollecita tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici.

In tale ottica assume rilevanza anche la nuova direttiva sulla protezione cibernetica e la sicurezza informatica nazionale emanata con DPCM del 17 febbraio 2017 (pubblicato sulla GU n. 87 del 13-4-2017) che si pone l'obiettivo di aggiornare la precedente direttiva del 24 gennaio 2013 e di conseguenza anche la relativa architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche.

L’esigenza di un nuovo provvedimento nasce innanzitutto dall’emanazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva NIS) recepita in Italia con il d.lgs. 18 maggio 2018, n. 65, nonché da quanto previsto dall'art. 7-bis, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge n. 198 del 2015, al fine di ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione della situazione di crisi, in relazione al grado di pregiudizio alla sicurezza della Repubblica e delle Istituzioni democratiche poste dalla Costituzione a suo fondamento.

I pericoli legati a questo genere di minacce sono particolarmente gravi per due ordini di motivi:
Il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati.
Il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti.

La combinazione di questi due fattori fa sì che misure tecniche adeguate, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongano l'accento sulle misure rivolte ad assicurare che le attività degli utenti rimangano sempre all'interno dei limiti previsti.
Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Naturalmente le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari dei dispositivi e dei software, che costituiscono le prime due classi di misure, nonché la protezione della configurazione (di hardware e software), che è quella immediatamente successiva.

La quarta classe deve la sua priorità alla duplice rilevanza dell'analisi delle vulnerabilità.
In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace.
Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.

La quinta classe è rivolta alla gestione degli utenti, in particolare con riferimento all'attività degli amministratori ed ad un uso appropriato dei relativi privilegi.

La sesta classe rappresentata dalle difese contro i malware deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.

Le copie di sicurezza, settima classe, sono alla fine dei conti l'unico strumento che garantisce il ripristino dopo un incidente.
L'ultima classe, la Protezione dei Dati, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

Ma tutto ciò ormai può anche non bastare, difatti sia le misure di sicurezza che le regole tecniche dovranno tener conto anche di quanto previsto dal GDPR che dedica molta attenzione agli aspetti di sicurezza.

L’art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento. Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Tali misure che non sono più minime o predeterminate comprendono:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il quadro desolante è che oggi, nonostante tutte queste problematiche, sono ben pochi gli enti pubblici che hanno avviato un percorso serio di adeguamento al GDPR.

Wolters Kluwer IPSOA Scuola di formazione

Gestione privacy in ambito comunicazioni elettroniche e controlli a distanza

Un tema che rimane sempre di grande attualità e di ampio contrasto tra gli addetti ai lavori è quello della vigilanza sulle comunicazioni elettroniche e sull'utilizzo di Internet sul posto di lavoro rispetto al quale si richiama il provvedimento generale dell'Autorità Garante per la protezione dei dati personali del 1 marzo 2007, il documento di lavoro delle autorità europee di protezione dei dati riunite nel Gruppo dei garanti europei, istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, adottato il 29 maggio 2002, nonché la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'articolo 8 della Convenzione europea dei diritti dell'uomo.

Ormai presso tutti gli uffici pubblici il collegamento ad Internet è molto diffuso, ma non bisogna dimenticare che l'uso di un computer collegato ad una rete esterna deve essere sempre molto accorto e responsabile innanzitutto per ovvie ragioni di sicurezza.

In un caso emblematico la Corte dei Conti - Sezione giurisdizionale per la regione Piemonte con sent. n. 1856/03 non ha esitato a condannare ad un congruo risarcimento del danno a favore dell'erario un dirigente pubblico reo di essersi collegato a siti Internet non istituzionali per una media di più di 2 ore al giorno.

Non poche, poi, sono le questioni sorte in merito alla legittimità dell'accesso da parte del datore di lavoro o dirigente alla casella di posta elettronica aziendale del dipendente.

Al fine di risolvere tali questioni è opportuno ricordare alcuni importanti concetti:

1. l'equiparazione della posta elettronica alla corrispondenza tradizionale la cui libertà e segretezza viene tutelata dall'art. 15 della Costituzione;
2. la legittimità o meno del controllo della casella della posta elettronica del proprio dipendente da parte del datore di lavoro alla luce di quanto prescritto dall'attuale disciplina in tema di rapporti di lavoro, compreso lo Statuto dei lavoratori;
3. la tutela della privacy alla luce di quanto stabilito dalla normativa comunitaria e nazionale.

La problematica non è semplice ed il Garante alla luce dei principi di cui sopra è intervenuto con un provvedimento nel quale ha chiarito che i datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali.

Spetta al datore di lavoro definire le modalità d'uso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali.

Ma cosa succede nel caso di messaggi inerenti al rapporto di lavoro? Anche in questo caso opera il divieto di controllo?

L'Autorità prescrive innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante vieta poi la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori (art. 4).

Viene inoltre indicata tutta una serie di misure tecnologiche e organizzative per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda.

Il provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

Il datore di lavoro è inoltre chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori.
Per quanto riguarda Internet è opportuno ad esempio:
- individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa;
- utilizzare filtri che prevengano determinate operazioni, quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali.

Per quanto riguarda la posta elettronica, è opportuno che l'azienda:
- renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
- valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
- preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi;
- metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.

Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

Il Garante ha chiesto infine particolari misure di tutela in quelle realtà lavorative dove debba essere rispettato il segreto professionale garantito ad alcune categorie, come ad esempio i giornalisti.

Diverso è il caso di richiesta di accesso di un dipendente a tutte le informazioni personali e le valutazioni professionali che lo riguardano, anche a quelle contenute nella posta elettronica dell'azienda. In tal caso l'azienda non può negare tale accesso, come precisato in precedenza, e per quanto non sia obbligata a esibire o copiare ogni documento, l'azienda deve comunque estrarre dagli atti tutte le informazioni relative al solo interessato e comunicargliele in modo facilmente comprensibile.

La videosorveglianza

In materia di rapporti fra privacy e videosorveglianza, al di là dei principi generali fissati dalla normativa comunitaria e nazionale in materia di protezione dei dati personali, bisogna fare riferimento ancora al provvedimento generale dell'Autorità Garante datato 8 aprile 2010 che ha sostituito il provvedimento generale del 29 aprile 2004 e fra poco interverranno anche le linee guida del Comitato Europeo sulla protezione dei dati personali.

Il provvedimento, ancora valido anche dopo il GDPR, purché compatibile, ha introdotto importanti novità in considerazione:
- dell'aumento massiccio di sistemi di videosorveglianza per diverse finalità (prevenzione, accertamento e repressione dei reati, sicurezza pubblica, tutela della proprietà privata, controllo stradale etc.);
- dei numerosi interventi legislativi adottati in materia: tra questi, quelli più recenti che hanno attribuito ai sindaci e ai comuni specifiche competenze, in particolare in materia di sicurezza urbana, così come le norme, anche regionali, che hanno incentivato l'uso di telecamere.

Principi generali

Il provvedimento del Garante ha dettato dei principi di carattere generale validi sia per i soggetti pubblici che per quelli privati adottati nel rispetto di quelle fondamentali prescrizioni in tema di privacy, di liceità, necessità, proporzionalità e finalità.

Innanzitutto è importante chiarire che l'installazione di telecamere è lecita solo se è proporzionata agli scopi che si intendono perseguire. Gli impianti di videosorveglianza devono essere attivati solo quando altre misure siano insufficienti o inattuabili.

Se è vero che il diritto alla protezione dei dati personali non pregiudica l'adozione di misure efficaci per garantire la sicurezza e l'accertamento degli illeciti è anche vero che l'installazione di sistemi di videosorveglianza non deve però violare la privacy dei cittadini e deve essere conforme al codice in materia di protezione dei dati personali.

La raccolta e l'uso delle immagini sono consentiti solo se fondati su presupposti di liceità: cioè, per i soggetti pubblici, quando siano necessari allo svolgimento di funzioni istituzionali e, per i privati, quando siano necessari per adempiere ad obblighi di legge o effettuate per tutelare un legittimo interesse.

L’informativa

I cittadini che transitano in aree sorvegliate devono essere informati con cartelli, visibili al buio se il sistema di videosorveglianza è attivo in orario notturno.
I sistemi di videosorveglianza installati da soggetti pubblici e privati (esercizi commerciali, banche, aziende etc.) collegati alle forze di polizia richiedono uno specifico cartello informativo, sulla base del modello elaborato dal Garante.
Le telecamere installate a fini di tutela dell'ordine e della sicurezza pubblica non devono essere segnalate, ma il Garante auspica l'utilizzo di cartelli che informino i cittadini.

Conservazione

Le immagini registrate possono essere conservate per periodo limitato e fino ad un massimo di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini di polizia e giudiziarie.

Per attività particolarmente rischiose (es. banche, videosorveglianza esercitata dai comuni per esigenze di sicurezza urbana) è ammesso un tempo più ampio, che non può superare comunque la settimana.

Ma ormai tutto dovrà essere valutato attentamente dal titolare del trattamento con l'ausilio del DPO.

Si ricorda che il provvedimento parlava di verifica preliminare (oggi non più esistente).

Settori di particolare interesse

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 tutela della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. La conservazione dei dati non può superare i 7 giorni, fatte salve speciali esigenze.

Sistemi integrati

Per i sistemi che collegano telecamere tra soggetti diversi, sia pubblici che privati, o che 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, sono obbligatorie specifiche misure di sicurezza (es. contro accessi abusivi alle immagini). Per alcuni sistemi è comunque necessaria la verifica preliminare del Garante.

Sistemi intelligenti

Per i sistemi dotati di software che permettono l'associazione di immagini a dati biometrici (es. "riconoscimento facciale") o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli (es. motion detection) è obbligatorio, alla luce del GDPR, la valutazione di impatto sulla protezione dei dati personali.

Violazioni al codice della strada

Sono obbligatori i cartelli che segnalano sistemi elettronici di rilevamento delle infrazioni. Le telecamere devono riprendere solo la targa del veicolo (non quindi conducente, passeggeri, eventuali pedoni). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo.

Deposito rifiuti

E’ lecito l’utilizzo di telecamere per controllare discariche di sostanze pericolose ed “eco piazzole”, per monitorare modalità del loro uso, tipologia dei rifiuti scaricati e orario di deposito.

Settori specifici

Luoghi di lavoro

Le telecamere possono essere installate solo nel rispetto delle norme in materia di lavoro. Vietato comunque il controllo a distanza dei lavoratori, sia all'interno degli edifici, sia in altri luoghi di prestazione del lavoro (es. cantieri, veicoli).

Ospedali e luoghi di cura

No alla diffusione di immagini di persone malate mediante monitor quando questi sono collocati in locali accessibili al pubblico. E' ammesso, nei casi indispensabili, il monitoraggio da parte del personale sanitario dei pazienti ricoverati in particolari reparti (es. rianimazione), ma l'accesso alle immagini deve essere consentito solo al personale autorizzato e ai familiari dei ricoverati.

Istituti scolastici

Ammessa l'installazione di sistemi di videosorveglianza per la tutela contro gli atti vandalici, con riprese delimitate alle sole aree interessate e solo negli orari di chiusura.

Taxi

Le telecamere non devono riprendere in modo stabile la postazione di guida e la loro presenza deve essere segnalata con appositi contrassegni.

Trasporto pubblico

E’ lecita l’installazione su mezzi di trasporto pubblico e presso le fermate, ma rispettando limiti precisi (es. angolo visuale circoscritto, riprese senza l’uso di zoom).

Tutela delle persone e della proprietà

Contro possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, sicurezza del lavoro ecc., si possono installare telecamere senza il consenso dei soggetti ripresi, ma sempre sulla base delle prescrizioni indicate dal Garante.

Come è noto, sempre in tema di videosorveglianza, l'art. 23, comma 1, del decreto legislativo n. 151/2015, (attuativo della legge delega n. 183/2014) ha modificato l'art. 4 dello Statuto dei Lavoratori ed in molti hanno gridato ad una vera e propria eliminazione del divieto di controllo a distanza dei lavoratori.

"1. 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.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 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."

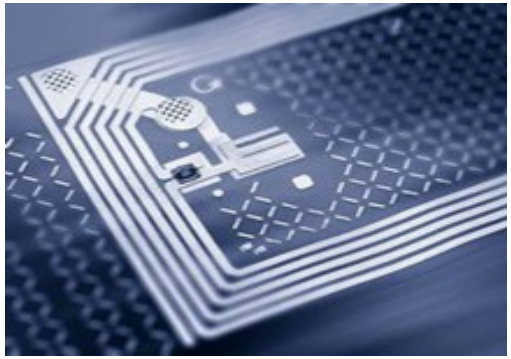
Ma la giurisprudenza della Corte di Cassazione già da un pò di tempo ha iniziato a rivedere l'applicazione dell'art. 4 dello Statuto dei Lavoratori. Difatti, con sentenza n. 4746 del 2002 la Cassazione ha escluso l'applicabilità di detto articolo ai controlli diretti ad accertare condotte illecite del lavoratore, i c.d. controlli difensivi. Il ragionamento della Corte, in tal senso, è chiaro: "Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 l. n. 300 citata, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o gli apparecchi di rilevazione di telefonate ingiustificate.

Successivamente, con la pronuncia n. 15892 del 2007, la Corte ha tuttavia ammesso un limite, affermando che i controlli difensivi non possono giustificare l'annullamento di ogni garanzia: "Né l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore".

Tale principio è stato riaffermato in numerose pronunce successive e, con la sentenza n. 4375 del 2010, è stato applicato anche ai programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet. La sentenza, dopo aver definito tale tipologia di controllo come "controllo preterintenzionale", rientrante perciò nell'ambito di applicazione del secondo comma dell'art. 4 dello Statuto dei lavoratori, ha affermato, quanto segue: "i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento".

Il Comitato Europeo per la protezione dei dati ha adottato di recente linee-guida sulla videosorveglianza (ancora non ufficiali), che chiariscono in quali termini il regolamento generale sulla protezione dei dati si applichi al trattamento dei dati personali quando si utilizzano dispositivi video, e mirano a garantire l'applicazione coerente del RGPD in materia. Le linee-guida riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti. Per quanto concerne questi ultimi, le linee-guida si concentrano sulle norme relative al trattamento di categorie particolari di dati. Altre tematiche affrontate nel documento riguardano, tra l'altro, la liceità del trattamento, l'applicabilità dei criteri di esclusione relativi ai trattamenti in ambito domestico e la divulgazione di filmati a terzi.

Rfid e Biometria



Tra le tecnologie innovative degli ultimi tempi che pongono non pochi problemi in tema di privacy rientrano senz'altro sia le RFID che i sistemi biometrici.

Rfid è un acronimo (Radio Frequency ID Devices) con cui si indicano dispositivi microscopici simili a microchip contenenti un identificativo (ad esempio, un numero di serie), che è possibile riconoscere attraverso un lettore compatibile funzionante in radiofrequenza.

Tali tecnologie si fondano sull'utilizzo di micro-processori che, collegati ad un'antenna ed impiegati come etichette di riconoscimento (*cd. etichette intelligenti*), sono in grado di trasmettere –attraverso onde radio– segnali leggibili da appositi lettori dotati di un'antenna di attivazione/ricezione.


1 Il lettore emette un campo magnetico o un segnale a radiofrequenza.
2 L'etichetta è alimentata dal segnale del lettore. Il circuito integrato attivato trasmette i dati che codifica.
Banca dati
Etichetta RFID
ENERGIA
DATI
Lettore RFID
3 Il lettore riceve i dati dell'etichetta e può interrogare la banca dati o semplicemente inviare il dato trasmesso dall'etichetta.
Ricerca:
Etichetta identificativa:
g231R525Q
Spedizione n.23
1200 unità
Asciugamani di carta
Partiti
Sigla identificativa dell'etichetta:
g231R525Q
ETICHETTA
DATI

La *Rfid* rappresenta uno strumento utile in numerosi settori e per diverse finalità: essa può essere impiegata, ad esempio, per il "tracciamento" di singole unità di prodotto nella catena di distribuzione dell'industria; per la prevenzione di furti e di contraffazioni dei prodotti; per garantire una maggiore rapidità nelle operazioni commerciali; per il controllo degli accessi ad aree riservate.

Ma attraverso le cd. “etichette intelligenti” si possono trattare, anche senza che l’interessato ne sia a conoscenza, innumerevoli dati personali che lo riguardano, compresi quelli di natura sensibile; raccogliere dati sulle abitudini del medesimo ai fini di profilazione attraverso l’aggregazione con altre informazioni di carattere personale; verificare prodotti (vestiti, accessori, medicine, ecc.) indossati o trasportati; tracciare i percorsi effettuati.

In questo settore il problema privacy sta diventando molto delicato perché tale tecnologia presenta enormi potenzialità: in prospettiva, anche in vista dell'ulteriore sviluppo tecnologico, dell'abbattimento dei costi di produzione, della possibilità di integrazione con altre infrastrutture di rete (telefonia, Internet, ecc.), le tecniche di identificazione via radio-frequenza potranno avere un impiego sempre maggiore e nei più diversi settori.

Occorre tenere altresì presente che più gravi pericoli per gli interessati possono derivare dal prevedibile incremento della potenza dei sistemi di *Rfid* (i quali potrebbero rendere fattibile una "lettura" delle etichette a maggiori distanze) nonché – specie in ragione dell'adozione di *standard* tecnici comuni – dalla possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, "riscrittura").

Per questi motivi il Garante ha svolto una prima attività di approfondimento della materia (provvedimento generale del 9 marzo 2005) rivolgendo l'attenzione al possibile impatto che le tecniche di identificazione via radio possono già avere sulle condizioni di esercizio delle libertà delle persone e alle problematiche che la loro introduzione è destinata a sollevare relativamente all'applicazione della normativa sulla tutela dei dati personali.

Del resto è notizia recente che l'obiettivo perseguito dalla Commissione europea attraverso una recente Comunicazione diffusa all'esito di una consultazione pubblica conclusasi nel 2006 è proprio una politica europea per i sistemi Rfid che coniughi l'esigenza di sfruttare le potenzialità di questa tecnologia con l'attenzione alla tutela della privacy ed ai possibili rischi per la salute e l'ambiente.

Tale obiettivo però non è stato seguito da una regolamentazione di carattere comunitario. Difatti Viviane Reding nel 2007 in qualità di Commissario Europeo per i media e la società dell'informazione, annunciò che la Commissione non avrebbe regolamentato la tecnologia Rfid, ma avrebbe permesso ai mercati di autoregolarsi.

I sistemi biometrici

Le tecnologie biometriche, consentono, mediante l'uso di specifici software e apparecchiature informatiche, il riconoscimento di un individuo attraverso dati fisici ricavati dall'analisi delle impronte digitali, della morfologia facciale e dal riconoscimento palmare.

Si tratta della ricerca più avanzata in tema di sicurezza degli accessi informatici. Alcune caratteristiche fisiche dell'utente autorizzato all'accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

Tra i sistemi biometrici si ricordano:

1. *le impronte digitali e le impronte palmari*;
2. *il riconoscimento della voce* (difettoso in caso di malattie da raffreddamento);
3. *il reticolo venoso della retina dell'occhio*;
4. *il controllo dinamico della firma* (con riferimento anche alla sua velocità di esecuzione).

Di fronte alla rapida ascesa di tali metodologie il Garante ha assunto, almeno all'inizio, un atteggiamento particolarmente rigido in quanto spesso le finalità di identificazione, sorveglianza, sicurezza delle transazioni non possono giustificare qualsiasi utilizzazione del corpo umano resa possibile dall'innovazione tecnologica.

Vanno garantiti sempre il rispetto della dignità della persona, il rispetto dell'identità personale, il rispetto dei principi di finalità e di proporzionalità ed infine la necessaria attenzione per gli effetti cosiddetti imprevisti o indesiderati e che, invece, spesso sono conseguenze determinate da analisi incomplete o troppo interessate delle tecnologie alle quali si intende ricorrere.

Ma ciò che più preoccupa è che il problema della protezione dell'identità dai suoi possibili "furti", già imponente nel settore del commercio elettronico, rischia di assumere aspetti preoccupanti con l'utilizzo della biometria.

Avuto, poi riferimento al mondo del lavoro, l'Autorità Garante nelle proprie "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" sottolineava che l'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non era lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta, partendo dal modello di riferimento, e la sua ulteriore "utilizzazione" a loro insaputa.

L'utilizzo di dati biometrici doveva, quindi, essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi venivano trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili", considerata la natura delle attività ivi svolte: si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore.

Inoltre, nei casi in cui l'uso dei dati biometrici era consentito, la centralizzazione in una banca dati delle informazioni personali (nella forma del predetto modello) trattate nell'ambito del descritto procedimento di riconoscimento biometrico risultava di regola sproporzionata e non necessaria.

In luogo, quindi, di modalità centralizzate di trattamento dei dati biometrici, doveva ritenersi adeguato e sufficiente avvalersi di sistemi efficaci di verifica e di identificazione biometrica basati sulla lettura delle impronte digitali memorizzate, tramite il predetto modello cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (una *smart card* o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale).

Si ricorda che successivamente, prima dell'avvento del GDPR, l'Autorità ha emanato il provvedimento generale in tema di biometria del 12 novembre 2014 di cui fanno parte integrante "Le linee guida in materia di riconoscimento biometrico e firma grafometrica" con le quali il Garante ha inteso fornire un quadro di riferimento unitario sulla cui base i titolari possano orientare le proprie scelte tecnologiche, conformare i trattamenti ai principi di legittimità stabiliti dal Codice, rispettare elevati standard di sicurezza.

Le prescrizioni

Oltre al principio di necessità va rispettato il principio di liceità (art. 6 del GDPR). Il trattamento mediante questi nuovi sistemi è lecito solo se si fonda su dei presupposti normativi che per i soggetti pubblici potrebbero essere lo svolgimento di funzioni istituzionali, mentre per i soggetti privati ed enti pubblici economici potrebbero essere l'adempimento ad un obbligo di legge, o consenso libero ed espresso.

Il titolare può trattare dati personali esclusivamente per scopi determinati, espliciti e legittimi *(art. 5 GDPR*). I dati possono essere inoltre utilizzati soltanto in termini compatibili con la finalità per la quale sono stati originariamente raccolti; devono essere conservati per il tempo strettamente necessario a perseguire tale finalità, decorso il quale devono essere cancellati o resi anonimi *(art. 5 GDPR)*.

Il titolare deve verificare il rispetto del principio di proporzionalità in tutte le diverse fasi del trattamento. I dati trattati e le modalità del loro trattamento, anche con riferimento alla tipologia delle infrastrutture di rete adoperate, non devono risultare sproporzionati rispetto agli scopi da prefissare.

Il titolare del trattamento, nel fornire agli interessati la prescritta informativa precisando anche le modalità del trattamento *(art. 13 del GDPR)*, deve indicare la presenza di etichette *RFID o sistemi biometrici* e specificare che, attraverso gli stessi strumenti è possibile raccogliere dati personali senza che gli interessati si attivino al riguardo.

Il titolare del trattamento deve agevolare l'esercizio, da parte dell'interessato, dei diritti di cui all'art. 15 e seguenti del GDPR, semplificando le modalità e riducendo i tempi per il riscontro al richiedente.

Si ricorda, però, che il Garante, con il menzionato provvedimento generale del 12 novembre 2014 aveva individuato alcune specifiche tipologie di trattamenti in relazione alle quali non riteneva necessaria la presentazione della predetta richiesta di verifica preliminare (oggi non più esistente), a condizione che fossero rispettati i presupposti di legittimità contenuti nel Codice e nelle linee-guida e che venissero adottate tutte le misure e gli accorgimenti tecnici descritti nel medesimo provvedimento.

I trattamenti in questione sono:

- autenticazione informatica;
- controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi;
- uso delle impronte digitali o della topografia della mano a scopi facilitativi;
- sottoscrizione di documenti informatici.

Naturalmente l'uso generalizzato della biometria, in virtù della delicatezza dei dati oggetto di trattamento, può presentare rischi per gli interessati, con potenziali gravi ripercussioni sulla loro sfera personale, in caso di impropria utilizzazione. E' necessario pertanto prevedere sempre un'accurata analisi dei rischi.

Il titolare del trattamento svolto con sistemi elettronici è tenuto ad adoperarsi, utilizzando i mezzi tecnici che lo stato dell'arte nel settore informatico rende disponibili, per proteggere i dati personali trattati con le misure di sicurezza una volta previste dal Codice, adesso dall'art. 32 del GDPR.

Il dato biometrico (usualmente in forma di modello biometrico, ma in alcuni casi anche di campione biometrico) può trovarsi nella disponibilità del titolare del trattamento ed essere conservato in un'unica banca dati centralizzata.
In alternativa, è possibile memorizzare il dato biometrico in dispositivi sicuri (es. token, smart card) affidati alla diretta ed esclusiva disponibilità degli interessati, in modo che il titolare non debba conservare il dato biometrico (template on card).

Proprio di recente, per l'esattezza il 19 settembre 2019, con provvedimento n. 167/2019 il Garante per la protezione dei dati personali ha fornito il proprio parere sullo schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo". In particolare lo schema di decreto ha assunto particolare rilevanza perché introduce i sistemi biometrici come strumento per combattere nel pubblico impiego i tristemente famosi "furbetti del cartellino".

L'Autorità nel proprio parere esprime notevoli perplessità in quanto innanzitutto la norma di legge (art. 2 legge n. 56/2019) che lo schema di regolamento è tenuto ad attuare presenti profili di dubbia compatibilità con la disciplina europea e nazionale in materia di protezione dei dati personali, come già rilevato dal Garante in sede di parere sullo schema di disegno di legge, nonché di audizione dinanzi alle Commissioni parlamentari competenti.
Sotto un primo profilo, infatti, la previsione dell'obbligatorio impiego contestuale di due sistemi di verifica del rispetto dell'orario di lavoro (raccolta di dati biometrici e videosorveglianza) contrasta con l'esigenza di stretta necessità del trattamento rispetto al fine perseguito; esigenza tanto più rilevante rispetto ai dati biometrici, annoverati nella categoria di dati personali cui la disciplina europea accorda maggiore tutela.
Per altro verso, la norma non sembra conforme a tali principi laddove intenda – come parrebbe dato il tenore letterale – configurare la rilevazione biometrica (unitamente peraltro alle videoriprese) quale obbligatoria in ogni pubblica amministrazione.

Wolters Kluwer IPSOA Scuola di formazione

Il Codice dell'Amministrazione Digitale

Come è noto tutte le norme - emanate per favorire la diffusione delle nuove tecnologie e l'ammodernamento delle strutture pubbliche – sono state raccolte in un codice approvato con *il decreto legislativo del 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione Digitale" (CAD).*

Quest'ultimo decreto legislativo ha subito diverse modifiche ed integrazioni: D. Lgs. 4 aprile 2006, n. 159, dalla legge 24 dicembre 2007, n. 244, dalla legge 28 gennaio 2009 n. 2, dalla legge 18 giugno 2009, n. 69, dalla legge 3 agosto 2009, dal d.lgs. 30 dicembre 2010, n. 235, dalla legge n. 221/2012 (recante i principi dell'Agenda Digitale), dalla legge n. 98/2013 (decreto del fare), dal d.lgs. n. 179 del 26 agosto 2016 ed infine dal d.lgs n. 217 del 13 dicembre 2017.

Con le ultime riforme non solo si è proceduto ad una modifica ed integrazione delle norme del CAD ma ne sono state abrogate diverse anche attraverso vari accorpamenti e semplificazioni.
L'obiettivo è innanzitutto quello di promuovere e rendere effettivi i diritti di cittadinanza digitale dei cittadini e delle imprese, garantendo, contestualmente, il diritto di accesso ai dati, ai documenti e ai servizi di loro interesse in modalità digitale, semplificando le modalità di accesso ai servizi alla persona e realizzando - come indicato dal titolo con cui è rubricato l'art. 1 della legge n. 124 del 2015 - una vera e propria "*carta della cittadinanza digitale*".

Altro obiettivo fondamentale è quello di spostare l'attenzione dal processo di digitalizzazione ai diritti digitali di cittadini e imprese. Con la "carta della cittadinanza digitale" si riconoscono direttamente diritti a cittadini e imprese e si costituisce la base giuridica per implementare Italia Login, la piattaforma di accesso che, attraverso il Sistema pubblico d'identità digitale (SPID) e l'Anagrafe nazionale della popolazione residente, permetterà ai cittadini di accedere ai servizi pubblici - e a quelli degli operatori privati che aderiranno - con un unico nome utente e un'unica *password* (prenotazioni di visite mediche, iscrizioni a scuola, pagamento dei tributi).

Il sistema SPID assume sempre di più un ruolo centrale in questo nuovo CAD e viene definito come un insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con specifico decreto ministeriale, identificano cittadini, imprese e pubbliche amministrazioni per consentire loro l'accesso ai servizi in rete.

Lo SPID, quindi, è un insieme di credenziali per accedere in rete a tutti i servizi della pubblica amministrazione e a quelli degli operatori commerciali che vi aderiranno. Lo SPID consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati per permettere ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano.

Con l'istituzione dello SPID le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi, oltre che con lo stesso SPID, solo mediante la carta d'identità elettronica e la carta nazionale dei servizi che alla fine avranno in tal senso una funzione solo residuale. La possibilità di accesso con carta d'identità elettronica e carta nazionale dei servizi resta comunque consentito indipendentemente dalle modalità predisposte dalle singole amministrazioni.

E’ chiaro, quindi, l’intento del legislatore di semplificare al massimo l’accesso ai servizi on line dei cittadini, superando le difficoltà connesse alle carte elettroniche, ma il pericolo “sicurezza” incombe sempre, poiché è evidente che con tale sistema si moltiplicano le identità digitali di un cittadino, che saranno diverse per ogni servizio e la prospettiva lascia perplessi. E’ anche vero che il sistema è continuamente monitorato dall’Autorità Garante giustamente preoccupata, ma è anche vero che se una singola identità digitale crea problemi figuriamoci tante.

Wolters Kluwer IPSOA Scuola di formazione

La gestione elettronica documentale

Lo sviluppo di strumenti quali la firma elettronica ed il protocollo informatico uniti all'espansione dell'uso della posta elettronica, rende possibile la realizzazione di una gestione completamente automatizzata dei flussi documentali e la conseguente attuazione di profonde innovazioni nelle modalità di lavoro delle unità organizzative.

La gestione documentale è la gestione informatica dei documenti in modalità avanzata. È stata così denominata perché si tratta di una soluzione che privilegia ed esalta essenzialmente le potenzialità legate alla gestione informatizzata dei documenti e degli archivi.

La gestione documentale consiste in realtà in una macro-categoria, che comprende attività assai eterogenee, che variano a seconda del grado di funzionalità che si desideri attuare, ma che trovano una logica ben precisa per il loro accorpamento: ovvero il loro comune presupposto fondamentale, che è quello della dematerializzazione dei documenti cartacei e quindi della disponibilità degli stessi a livello informatico.

Le fasi del documento informatico

FORMAZIONE
(originale informatico, copia per immagine, copia informatica, duplicato)

Integrità, immodificabilità, autenticità

GESTIONE DOCUMENTALE
(protocollo - registrazione e segnatura di protocollo, classificazione, organizzazione e fascicolazione, assegnazione, reperimento)

Contestualizzazione, archiviazione, ricercabilità

CONSERVAZIONE
(verifica, consolidamento, mantenimento leggibilità nel tempo, sicurezza)

Le Regole Tecniche

La dematerializzazione dei documenti cartacei prevede le seguenti attività:
-registrazione con trattamento delle immagini (scannerizzazione dei documenti cartacei);
-assegnazione per via telematica al destinatario;
-gestione avanzata della classificazione dei documenti (utilizzo di *thesauri* e vocabolari controllati ecc.);
-collegamento dei documenti alla gestione dei procedimenti.

E’ indispensabile, inoltre, ai fini di una valida ed efficace informatizzazione delle attività di un ufficio, la cd. reingegnerizzazione dei processi interessati (in altri termini adeguare le procedure amministrative alle esigenze dell’informatizzazione).

Appare, quindi, chiaro che la vera dematerializzazione in realtà non può ridursi ai processi di digitalizzazione dei documenti, bensì consiste nel faticoso e complesso intervento di semplificazione dei processi e di diminuzione delle fasi e dei passaggi del processo decisionale, come del resto indicato negli obiettivi della legge 241 del 1990 da ormai 20 anni.

Bisogna, però, chiarire che la dematerializzazione o meglio il processo di informatizzazione della memoria documentaria, deve includere inoltre, per produrre risultati di qualche efficacia, il controllo sulla corretta formazione del documento e il governo del ciclo del documento in tutte le sue fasi incluso quello della conservazione: nessun processo di trasformazione può avere successo se non prevede la definizione di procedure e il controllo gestionale pianificato di tutte le fasi.

Riguardo la conservazione sostitutiva dei documenti informatici, l'art. 43 del CAD sancisce che gli obblighi di conservazione e di esibizione di documenti si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle linee guida.

In particolare al comma 1-bis dell'art. 44 del CAD si introduce la figura del responsabile della gestione dei documenti informatici che deve operare d'intesa con il responsabile della transizione al digitale, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196 (ora superato), ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza.

Inoltre al comma 1-quater dell'art. 44 del CAD si prevede la possibilità per il responsabile della conservazione, che opera a sua volta d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, di chiedere la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche e di protezione dei dati personali.

Wolters Kluwer IPSOA Scuola di formazione

Government 4.0: gestire l'innovazione della PA

La novità di maggior rilievo dal punto di vista giuridico-tecnologico della recente conversione in legge n. 12/2019, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione è sicuramente rappresentata dall'art. 8-ter dove vengono definite le tecnologie basate sui registri distribuiti e gli smart contract.

Per smart contract si intende "un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse". Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

Indubbiamente è encomiabile il tentativo del legislatore di definire queste nuove tecnologie fortemente incentivate dalla stessa commissione europea, basti vedere alla Risoluzione del Parlamento europeo del 3 ottobre 2018 o anche al Libro bianco "Raccomandazioni per adottare standard comuni in Europa sulla Blockchain e sui registri distribuiti (distributed ledger)", a cura del Comitato europeo per la standardizzazione (Cen) e del Comitato europeo per la standardizzazione elettronica (Cenelec) che affronta la delicata problematica dei requisiti che dovranno avere i servizi basati sulle nuove tecnologie blockchain per abilitare servizi sicuri e di qualità.

La blockchain sostanzialmente è:

- Una «catena di blocchi» che crea un registro digitale. Le operazioni, come un atto di compravendita o transazioni in moneta virtuale, vengo vagliate da molteplici operatori che ne garantiscono l'autenticità.
- Un database (registro) distribuito per la gestione di transazioni crittografate ed è aperta a tutti.
- Il database è composto da una serie di blocchi che archiviano un insieme di transazioni validate dai nodi della catena.
- La catena è composta da nodi, transazioni, blocchi, ledger/registri, funzioni di hash.
- Le transazioni, verificata la loro correttezza, vengono archiviate su tutti i nodi della blockchain.

Le tecnologie utilizzate sono:

- Database distribuito.
- Funzioni di hash.
- Crittografia asimmetrica.
- Firma digitale (ECDSA – curve ellittiche).
- Timestamping

Come funziona?

- Due soggetti vogliono effettuare una transazione.
- Sono noti gli indirizzi dei soggetti e la transazione contiene le informazioni necessarie per completarla e validarla.
- Le chiavi asimmetriche sono utilizzate per firmare la transazione (la privata) e per creare l'indirizzo del soggetto (la pubblica).
- La funzione di hash viene utilizzata per garantire l'integrità dei blocchi, la loro concatenazione e per creare l'ID del soggetto.
- Il timestamping viene calcolato in modo «mediano». Questo perché la transazione (inserita in un blocco di transazioni) deve essere verificata e approvata dai partecipanti alla blockchain.
- Dopo la verifica e validazione (Proof Of Work - mining) il blocco è aggiunto alla catena e ne diventa parte immodificabile. Il database dei blocchi è distribuito e concatenato.

La grande sicurezza, trasparenza e versatilità dello strumento sta vincendo le iniziali resistenze di molti operatori ed ormai sono diversi i campi di utilizzazione della blockchain.

Le criticità

Gli Smart Contract potrebbero essere una risorsa molto importante nella gestione dei documenti presenti nel procedimento amministrativo della PA per le loro caratteristiche di sicurezza e trasparenza, per quanto allo stato attuale dell'arte gli stessi Smart Contract risultano avere dei problemi legati alla struttura pubblica e decentralizzata della blockchain, nel tempo stesso punto di forza e di debolezza della stessa.

Per quanto riguarda i dati pubblici è necessario ed importante tutelare la loro natura pubblica. Contemporaneamente è altrettanto determinante salvaguardare la tutela della privacy, ovvero la natura confidenziale, delle informazioni trattate. Queste caratteristiche, tanto importanti quanto opposte, mal si conciliano con lo stato attuale dello sviluppo tecnologico degli Smart Contracts su Blockchain rendendone l'utilizzo, ad oggi, complesso e costoso.

D’altronde come sottolineato dal Parlamento Europeo nella stessa Risoluzione è opportuno che, per tali tecnologie di registro, si affrontino adeguatamente anche le problematiche attinenti proprio al settore della protezione dei dati personali dove il Regolamento europeo n. 2016/679 ha introdotto importanti principi come quello di accountability o il principio della privacy by design che diventa fondamentale con riferimento alla blockchain.

La presenza di dati personali all'interno di un sistema contraddistinto dalla tecnologia di registro può creare non pochi problemi in merito al rispetto dell'attuale normativa comunitaria poiché diventerebbe, innanzitutto, difficilmente gestibile la presenza di errori con riferimento agli stessi dati che rappresentano il logico presupposto di una "catena" davvero poco elastica per ragioni di sicurezza. Inoltre per le stesse ragioni, come è noto, poiché il dato personale non può essere conservato per sempre, l'eventuale cancellazione nel rispetto del GDPR diventerebbe non poco difficoltosa.

La predisposizione di un sistema contraddistinto da tale tecnologia implica, inevitabilmente, nell'ottica dei principi generali del GDPR sopra evidenziati, uno studio approfondito sui rischi, non di poco conto, connessi in materia di protezione dei dati personali per cui sarebbe necessario quanto meno condurre un'accorta valutazione di impatto sulla protezione dei dati personali alla luce dell'art. 35 del GDPR che tenga conto delle specifiche peculiarità dello strumento tecnologico.

In altri termini è giusto come sottolineato dalla Commissione europea studiare ed approfondire tali tecnologie ma non giungere a conclusioni troppo affrettate visto che il nostro paese ha già vissuto precedenti esperienze vedi la firma digitale o la posta elettronica certificata dove ha anticipato l'introduzione e la regolamentazione di tecnologie rimanendo però drammaticamente isolato per la mancata condivisione nell'ambito dell'Unione europea.