FONDAZIONE ROMAGNOSI
Scuola di governo locale

Quaderni della Fondazione Giandomenico Romagnosi

Quaderno 1/2024

La Protezione dei dati personali nella p.a.: opportunità e criticità

Autori:

Raffaella Procaccini

Tiziana Santoro

Marzo 2024

Quaderno Romagnosi 1/2024, marzo 2024.
La Protezione dei dati personali nella p.a.: opportunità e criticità.
Autori: Raffaella Procaccini e Tiziana Santoro.

La Protezione dei dati personali nella p.a.: opportunità e criticità

Autori:

Raffaella Procaccini[1]

Tiziana Santoro[2]

[1] Avv. Raffaella Procaccini, membro del Comitato Scientifico della Fondazione Romagnosi.

[2] Dott.ssa Tiziana Santoro, funzionaria della pubblica amministrazione, ha conseguito il titolo di Master di II livello dell'Università degli Studi di Pavia in "Amministrazione territoriale e politiche di sviluppo locale" (I edizione, a.a. 2020-2021).

INDICE

Premessa.

Il presente contributo nasce dall'interesse sentito in ordine all'argomento della protezione dei dati da parte della p.a. nelle more dei corsi di formazione tenuti dalla Fondazione Romagnosi.

E' evidente che con l'introduzione dello *smart working* e con l'implementazione dell'utilizzo dei sistemi informatici il tema della conservazione dei dati e delle modalità di diffusione è sempre più importante.

In ogni caso l'esigenza della protezione dei dati non deve rallentare l'agire della p.a. o rendere oscura l'informazione che il privato richiede alla p.a.

Purtroppo, dall'esame dei casi pratici emerge che nella valutazione del rischio non esiste un rischio zero di possibile lesione della protezione dei dati ma di certo uno strumento di prevenzione è individuare i possibili rischi, individuare i soggetti responsabili a fini preventivi nonché formare sull'importanza di applicare in modo corretto il principio di minimizzazione dei dati, il principio di esattezza e di necessaria valutazione preliminare d'impatto.

Avv. Raffaella Procaccini

1. L'importanza della tutela dei dati personali.

di Raffaella Procaccini

Una premessa normativa diviene doverosa. La normativa sulla protezione dei dati personali persegue la finalità di tutelare le persone fisiche dalla lesione che potrebbe loro derivare in sede di trattamento di tali dati. All'interno delle Pubbliche Amministrazioni, è necessario, ovviamente, operare un bilanciamento tra l'esigenza di garantire il buon andamento della Pubblica Amministrazione, principio cristallizzato nell'art. 97 della Costituzione, e la tutela dei diritti del privato cittadino.

L'importanza della tutela dei dati si ravvisa, all'interno dalla p.a., in diversi ambiti: pensiamo, ad esempio, al dipendente pubblico che debba fornire, a mezzo mail, una risposta al privato cittadino, ovvero al messo notificatore che debba effettuare una notifica al privato. Su tale ultimo punto, è interessante approfondire il tema circa la necessità o meno che il messo notificatore sia identificabile dal privato all'atto della notifica.

Prima di tale approfondimento, è opportuno soffermarsi brevemente sulla figura del messo comunale e del messo notificatore.

Il messo comunale ha competenza generale alla notifica degli atti delle Pubbliche Amministrazioni individuate dall'art. 1 del D.lgs. 165/2001: egli è nominato con atto del Responsabile del Servizio, in ottemperanza all'art. 107 del D.lgs. n. 267/2000, e ricopre l'incarico di pubblico ufficiale – in quanto tale, è tenuto ad osservare gli obblighi di diligenza, lealtà ed imparzialità che qualificano il corretto adempimento della prestazione lavorativa alle dipendenze della Pubblica Amministrazione.

La Legge finanziaria del 2007 (L. 296/2006) all'art. 1, commi 158, 159 e 160, introduce una nuova figura: si tratta del messo notificatore, con specifiche competenze per la notificazione delle ingiunzioni fiscali. Tali soggetti possono essere nominati tra il personale dipendente del Comune, al fine di notificare gli atti inerenti al recupero delle entrate tributarie ed extra-tributarie del proprio ente. L'esclusiva qualifica di messo notificatore non consente la notifica di tutti gli altri atti, interni ed esterni, se non nell'unica ipotesi in cui lo stesso soggetto sia anche stato nominato messo comunale.

Ciò premesso, in tema di trattamento dei dati personali dei dipendenti delle Pubbliche Amministrazioni, come sopra rilevato, sorge l'esigenza di

bilanciare il principio di trasparenza della p.a. con il rispetto della riservatezza del privato cittadino – che qui assume anche le vesti di pubblico dipendente.

A tale scopo, nel giugno del 2007, è intervenuta l'Autorità Garante della Privacy, dettando apposite Linee guida[3], sulla scorta di quanto già indicato nel D.lgs. 165/2001 ("*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*") e di quanto già stabilito con riguardo al rapporto lavorativo privato (Deliberazione Garante della Privacy n. 53 del 23 novembre 2006), di cui si applicano i principi, salvo opportune deroghe.

L'art. 55-novies del D.lgs. 165/2001, introdotto dall'art. 69 del D.lgs. 150/2009, stabilisce che «i dipendenti delle Amministrazioni Pubbliche che svolgono attività a contatto con il pubblico sono tenuti a rendere conoscibile il proprio nominativo mediante l'uso di cartellini identificativi o di targhe da apporre presso la postazione di lavoro».

Da tale obbligo, come precisa il comma successivo del richiamato articolo, sono escluse determinate categorie individuate da ciascuna amministrazione.

Al fine di chiarire e specificare il contenuto della norma sopra richiamata, è stata pubblicata la Circolare n. 3 del 2010 del Dipartimento della Funzione Pubblica[4]. La stessa precisa che, con riferimento all'inciso dell'art. 55-novies del D.lgs. 165/2001, secondo il quale il riconoscimento può avvenire tramite cartellini identificativi o di targhe da apporre presso la postazione di lavoro, la scelta tra le due modalità è rimessa alle singole amministrazioni in relazione alla tipologia di attività svolta, ferma restando la possibilità di adottare entrambe le modalità identificative. In ogni caso, si tratta di un "contenuto minimo" di riconoscimento, perciò l'amministrazione può valutare se e quando esporre e specificare ulteriori elementi identificativi del dipendente pubblico, nei limiti della diffusione di dati personali non pertinenti o eccedenti la finalità perseguita (così, art. 11 del D.lgs. 196/2003).

Così – come chiarito dalla Circolare a titolo esemplificativo – esorbita dalle finalità identificative l'indicazione delle generalità del dipendente, come la data di nascita, atteso che per il suo riconoscimento è sufficiente il nominativo ovvero il codice dello stesso [5].

[3] https://www.garanteprivacy.it/

[4] https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/

[5] In relazione ad eventuali reclami del pubblico dipendente si rende utile citare quale spunto di riflessione la seguente statuizione. Con Provvedimento del 18 ottobre 2012, il Garante della Privacy ha rigettato il reclamo di una dipendente INPS che aveva lamentato una violazione dei propri dati personali (richiamandosi alle Linee guida) dopo che le erano state trasmesse, con modalità che avevano favorito la conoscenza, da parte di soggetti terzi, di informazioni personali, nonché un'asserita fuga di notizie, due note dirigenziali sul mancato raggiungimento degli obiettivi annuali. Il Garante rilevò che, in relazione alle modalità di trasmissione delle note, queste fossero state consegnate da un'incaricata assegnata alla segreteria della dirigente firmataria, che poteva legittimamente prenderne conoscenza nello svolgimento delle proprie attribuzioni. Da ciò consegue che la trasmissione delle note oggetto di reclamo era avvenuta ad opera di personale incaricato del trattamento. Il Garante della Privacy ha quindi concluso che, nel caso di specie, non ricorreva alcuna violazione della disciplina di protezione dei dati personali.

Ciò viene altresì ribadito nelle già menzionate *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati* (Deliberazione Garante della Privacy n. 53 del 23 novembre 2006), ai sensi delle quali, in relazione al rapporto con il pubblico, si è considerata sproporzionata l'indicazione sul cartellino di dati personali identificativi (generalità o dati anagrafici), ben potendo spesso risultare sufficienti altre informazioni (quali codici identificativi, il nome o il ruolo professionale), per sé sole in grado di essere d'ausilio all'utenza.

A tali regole sono sottratti i dipendenti pubblici di cui all'art. 3 del D.lgs. 165/2001 (personale in regime di diritto pubblico), nonché altre specifiche categorie di lavoratori pubblici, come per esempio gli operatori sanitari, per i quali, alla luce di specifiche esigenze di personalizzazione e di umanizzazione del servizio e/o di collaborazione, è consentito riportare nei cartellini elementi identificativi ulteriori rispetto alla qualifica, al ruolo professionale, alla fotografia o ad un codice identificativo, come le proprie generalità.

Da ultimo, occorre segnalare che, ai sensi delle citate Linee guida, non è in ogni caso consentito utilizzare in modo generalizzato sistemi di rilevazione automatica delle presenze dei dipendenti mediante la raccolta di dati biometrici, specie se ricavati dalle impronte digitali; ne deriva che tale operazione deve escludersi altresì quando la raccolta dei dati sia funzionale all'identificazione da parte di soggetti terzi.

In conclusione, in qualità di dipendenti della Pubblica Amministrazione a contatto con il pubblico, nulla osta al riconoscimento dei messi notificatori di un Comune per il tramite di un cartellino identificativo indicante il nome, il ruolo e/o un codice di riferimento, mentre sono esclusi, secondo le Linee guida del Garante della Privacy, altri dati inerenti la persona, la cui esposizione non è necessaria alle finalità in discorso, come le altre generalità del dipendente ovvero i suoi dati biometrici.

I suddetti argomenti sono utili per sottolineare come da un lato è importante la tutela della protezione dei dati, ma dall'altro va attuato un necessario bilanciamento degli interessi tra pubblico e privato.

2. I responsabili della tutela.

di Raffaella Procaccini

Come indicato in premessa, a fini preventivi è necessario responsabilizzare coloro che vengono individuati come destinatari di eventuali sanzioni in caso di lesione dei dati personali.

Secondo l'art. 1 della Legge n. 675/1996, il **"titolare del trattamento"** dei dati è la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le scelte di fondo sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza. Il riferimento alla "*persona fisica*" non riguarda coloro che amministrano o rappresentano la persona giuridica, la pubblica amministrazione o l'ente, ma concerne gli individui che effettuano un trattamento di dati a titolo personale (ad esempio, il libero professionista, il piccolo imprenditore), e che assumono individualmente la piena responsabilità di un'attività che va distinta nettamente, anche sul piano giuridico, da quella che singole persone fisiche possono coordinare nell'ambito e nell'interesse di una persona giuridica, di un'impresa o di un ente nel quale ricoprono incarichi di rilievo.

Pertanto, qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "*titolare*" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.) anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno.

Ai sensi dell'art. 25 del GDPR, il titolare del trattamento è intimato a porre in atto «tutte le misure per garantire che siano che siano trattati, per **impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento»[6].

[6] Per citare alcuni casi noti, in Italia l'art. 25 è stato richiamato nel Provvedimento del 2021 ai danni di: Istituto Nazionale di Previdenza Sociale (INPS), sanzione di 300.000€; Aeroporto Guglielmo Marconi di Bologna, sanzione di 40.000€ e al suo fornitore software € 20.000 (il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare la conformità ai principi di protezione dati impartendo le necessarie istruzioni al fornitore del servizio - ad es. disattivando le funzioni in contrasto con le norme di settore); Comune di Palermo, sanzione di 40.000€ per violazione del principio di "integrità e riservatezza", in quanto non è stata assicurata un'adeguata sicurezza dei dati personali, avendo consentito accessi non autorizzati; ma anche per violazione dei principi "di protezione dei dati fin dalla progettazione" non avendo messo in atto adeguate misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, nonché a garantire che non siano resi accessibili dati personali a un numero indefinito di persone fisiche; ed infine per violazione dell'art.

I dati sensibili devono essere pertanto resi accessibili a un numero limitato di soggetti – ne discende che, in ottemperanza al principio di sicurezza dei dati personali, è lecito il mascheramento di dati personali e superflui alle finalità del trattamento, così come previsto dall'art. 44 del GDPR[7].

Soggetto diverso dal titolare del trattamento è il **"responsabile per la protezione dei dati"**: trattasi di una figura professionale esperta nella protezione dei dati, il cui compito è valutare e organizzare la gestione del trattamento dei dati personali, e dunque la loro protezione, all'interno di enti come un'impresa, un ente o di un'associazione, affinché questi siano trattati in modo lecito e pertinente. In ultima analisi, il responsabile per la protezione dei dati affianca il titolare e/o il responsabile del trattamento per le funzioni di supporto, controllo e prassi formative e informative sulle disposizioni previste dal GDPR: egli agisce come rappresentante del Garante della Privacy nell'organizzazione.

Terza figura di rilievo nell'analisi dei soggetti coinvolti nel trattamento dei dati personali è il **"responsabile del trattamento":** in base alla normativa vigente[8], il Responsabile del trattamento dei dati personali è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

Per (poter) essere qualificati responsabili del trattamento occorre che il trattamento di dati personali avvenga "per conto" del titolare, nel senso che il soggetto deve trattare i dati personali a beneficio del titolare del trattamento: in questa sede, agire "per conto di" significa che il responsabile del trattamento non può effettuare trattamenti per proprie finalità. Le finalità e i mezzi del trattamento, infatti, devono essere sempre (e solo) stabilite dal titolare del trattamento. Si ricorda però che il titolare del trattamento anche quando utilizza prodotti da terzi deve verificare (si pensi, ad esempio, al caso in cui l'acquisizione e la gestione delle segnalazioni di illeciti avveniva senza l'uso di un protocollo di rete sicuro e che l'applicativo stesso non preveda la cifratura dei dati identificativi).

La sensibilità intrinseca ai dati personali espone l'attività di trattamento a un rischio, quello della violazione dei dati, qui sintetizzabile come l'impatto negativo sulle libertà e i diritti degli interessati (non solo il diritto alla protezione dei dati personali, ma anche altri, come la libertà di espressione[9]).

32 del Regolamento, data l'assenza di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, in quanto non si è tenuto conto dei rischi di accessi non autorizzati.

[7] "Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato".

[8] GDPR, art. 4, par. 1, n. 8.

[9] Per una più esaustiva definizione del concetto di rischio, si rimanda al Considerando 75 del GDPR.

Per violazione dei dati, il GDPR intende ogni «violazione di sicurezza che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» dal titolare del trattamento.

Per fronteggiare tali violazioni (c.d. *data breach*), il GDPR prevede una procedura che si può articolare come segue: a) rilevazione di una potenziale violazione dei dati; b) prima valutazione della notizia di violazione; c) misure immediate per risolvere o mitigare i rischi; d) valutazione dell'entità del rischio; e) notifica della violazione all'autorità di controllo e comunicazione agli interessati; f) tracciatura nel Registro delle violazioni.

Si noti che la normativa non prevede una sanzione automatica in caso di violazione dei dati all'interno dell'organizzazione, essendo necessario, a tal fine, che il Garante provveda (verosimilmente, quando sollecitato dagli interessati) all'adozione di eventuali misure correttive e sanzioni pecuniarie per i casi più gravi. Si considerino, poi, le fattispecie di reato introdotte dal D.lgs. 196/2003 agli artt. 167-171[10].

Possiamo, quindi, così riassumere i punti fondamentali della disciplina posta a tutela del trattamento dei dati personali: a) *minimizzazione dei dati* (non raccogliere più dati del necessario[11]); b) *limitazione delle finalità*[12] (non trattare i dati per scopi diversi da quelli stabiliti); c) *limitazione della conservazione* (non mantenere i dati quando non sono più necessari).

[10] Trattamento illecito dei dati, Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala, Acquisizione fraudolenta dei dati personali oggetto di trattamento su larga scala, Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o poteri del Garante, Inosservanza di provvedimenti del Garante, Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

[11] Si pensi al caso in cui l'istituto non si limiti a raccogliere da fonti quali banche dati ma coinvolga in modo indiscriminato.

[12] Sul sito web istituzionale di un Comune era liberamente visualizzabile un documento relativo all'atto di citazione dinnanzi al Tribunale di Taranto, contenente chiare informazioni personali del reclamante. In questa sede il Garante ha confermato, con ordinanza di ingiunzione del 5 marzo 2020, l'illiceità del trattamento dei dati personali effettuata dal Comune, in quanto la diffusione via web avveniva senza alcun presupposto normativo e in quanto la diffusione del nominativo non risultava necessaria rispetto le finalità del trattamento.
Considerato che nell'immediato il Comune rimuoveva tali dati dal sito istituzionale, si ritenevano non applicabili altre misure correttive.

3. La valutazione d'impatto ai sensi dell'art. 35 GDPR.

di Raffaella Procaccini

Dati i sopra indicati argomenti ai fini di un efficace bilanciamento tra interessi privati e pubblici diviene protagonista la valutazione d'impatto.

Ai sensi dell'art. 35 del Reg. 679/2016 (c.d. GDPR) si prevede letteralmente che:

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta, in particolare, nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1[13], o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Ai sensi dei paragrafi 7, 8, 9 e 10:

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

[13] Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto, da parte di questi ultimi, dei codici di condotta approvati di cui all'articolo 40[14], in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e)[15], trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

A seguito di tale premessa normativa, è opportuno soffermarsi, nella specie, su alcuni casi concreti per comprenderne l'importanza quali, ad esempio, l'apposizione di sistemi di videosorveglianza nei pressi di edifici comunali.

La liceità dell'acquisizione dei dati personali da parte di autorità competente, anche attraverso sistemi di videosorveglianza, è ricondotta agli artt. 1, 5 e 6 del Decreto-legge del 18 maggio del 2018, n. 51, con cui si attua nell'ordinamento interno la Direttiva (UE) del 27 aprile 2016, n. 680, in materia di *protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti*.

L'art. 5 del Decreto 51/2018 prevede che «il trattamento è lecito se è necessario per l'esecuzione di un compito di un'autorità competente a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali» - finalità alle quali si aggiungono, a norma dell'art. 1, Par. 1, della Direttiva 680/2016 «la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

[14] Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente Regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.
[15] Ci si riferisce ai casi in cui: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Pertanto, tali disposizioni rilevano l'importanza teleologica dell'acquisizione e del trattamento dei dati personali, escludendo, quindi, i casi esuberanti dalle finalità predette; infatti, in caso di trasmissione o acquisizione illecita o inesatta, il destinatario ne deve essere tempestivamente informato e i dati devono essere rettificati o cancellati a norma dell'art. 4, Paragrafo 3, del D.lg. 51/2018.

Tali procedimenti e cautele si applicano in favore del *principio di salvaguardia e protezione dei dati personali* e *di tutela dell'interessato*, attorno ai quali viene costituita la normativa fin qui citata.

Con riguardo al caso concreto prima citato, si rileva che, ai sensi della Legge del 23 aprile 2009, n. 38, *in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*, commi 7 e 8 dell'art. 6, titolato "*Piano straordinario di controllo del territorio*", il Comune ha il diritto di installare sistemi di videosorveglianza ai fini della sicurezza pubblica in luoghi pubblici o aperti al pubblico, quale l'ingresso di un edificio comunale. Inoltre, si prevede una conservazione della registrazione limitata a sette giorni che si adegua, evidentemente, alle finalità per cui è previsto il sistema di videosorveglianza.

Come riporta il Paragrafo 7 dell'art. 3, titolato *Trattamento dei dati personali per le finalità istituzionali dell'impianto di videosorveglianza*, del Regolamento di Videosorveglianza approvato dal Consiglio Comunale di Testico[16]:

> L'impianto di videosorveglianza non potrà essere utilizzato, in base all'art. 4 dello Statuto dei lavoratori (Legge 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'Amministrazione comunale, di altre Amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Pertanto, si riconosce come un sistema di videosorveglianza debba fungere, in un luogo pubblico (come l'ingresso di un edificio comunale), solo da deterrente o sistema di controllo per l'eventualità di reati o atti illeciti, senza minare le libertà civili né degli utenti né dei dipendenti.

Un altro tema interessante, legato a quello della videosorveglianza, concerne l'utilizzo di *bodycam* sugli operatori delle forze di polizia (in particolare, i Reparti mobili della Polizia di Stato). Al riguardo, risultano interessanti i Pareri del Garante del 22 luglio 2021 nn. 290 e 291[17]. In tali atti,

[16]https://www.gazzettaamministrativa.it
[17] https://all-in-giuridica.seac.it/

il Garante dispone che ogni *bodycam* sia ricondotta, attraverso l'identificativo della telecamera, all'operatore a cui è affidata, attraverso un registro prontamente compilato prima dell'attività operativa. L'avvio delle registrazioni deve essere disposto unicamente dall'ufficiale di pubblica sicurezza responsabile incaricato, o dai componenti della squadra, laddove sussista la necessità immediata della ripresa. È, quindi, vietata la registrazione di immagini o scene che non siano caratterizzate da criticità nel contesto operativo in cui si adottano i dispositivi. Pertanto, il Paragrafo 8 dell'art. 2 del parere n. 290[18] afferma:

> Le registrazioni avviate accidentalmente, in mancanza del requisito della necessità o avviate in previsione dell'insorgenza di situazioni "critiche" che non si siano poi verificate, sono cancellate tempestivamente dagli "amministratori di sistema" nazionali a seguito della formale richiesta dell'Ufficiale di pubblica sicurezza responsabile del servizio, inviata da questi nel più breve tempo possibile.

La giurisprudenza italiana e il Garante non si sono, invece, ancora espressi in merito all'uso delle *dashcam*[19] da parte di Autorità di Polizia; per questo motivo si può portare alla luce una sentenza del Bundesgerichtshof tedesco civile, equivalente della Corte di Cassazione per l'Italia, del 15 maggio 2018, n. VI ZR 233/17[20]. Essa ha riconosciuto l'ammissibilità e l'utilizzabilità delle *dashcam* da parte dell'Autorità Competente, pur sempre nell'applicazione dei principi del GDPR e, pertanto, consigliando l'attivazione della registrazione tramite sensore di movimento, in caso di collisione o di forte decelerazione del veicolo, così da non acquisire registrazioni costanti per il perdurare dell'attività operativa.

È interessante analizzare anche il tema delle c.d. fototrappole[21]. Si rinvengono, in materia, delle autorizzazioni all'impiego di tali dispositivi nella Delibera del Consiglio regionale Lombardia del 15 giugno 2021, n. XI/1908[22], e nel Comitato interministeriale per la programmazione economica del 03 agosto 2011, n. 57[23]. Per quanto concerne la programmazione economica del Comitato interministeriale, si riconduce la finalità d'impiego delle fototrappole,

[18] https://all-in-giuridica.seac.it/
[19] Dashcam è l'abbreviazione di "dashboard camera" ("dashboard" in inglese significa cruscotto): si tratta, dunque, di piccole videocamere che vengono installate sul cruscotto di un'automobile al fine di registrare le immagini della strada, durante la sosta o la guida.
[20] https://juris.bundesgerichtshof.de/
[21] Si tratta di vere e proprie telecamere di sicurezza, dotate di sensore di movimento, che riescono a scattare fotografie o registrare video nel momento in cui viene allertata dal passaggio di persone o animali.
[22] https://www.assorecuperi.it/
[23] https://leg16.camera.it/

per almeno tre anni, di monitoraggio dei punti critici della rete ferroviaria e stradale. La D.c.r. richiama, invece, un'altra D.c.r. del 28 luglio 2020, n. XI/1113, valutante il sostegno finanziario agli enti locali per l'acquisto di fototrappole per il monitoraggio finalizzato al controllo dello scarico abusivo di rifiuti.

Di particolare nota è la sentenza della Corte di Cassazione penale del 18 aprile 2023, n. 36696, che condanna l'imputato alla reclusione di anni uno e mesi quattro per il delitto di incendio boschivo doloso, grazie alle immagini acquisite da una fototrappola, installata nella zona per la prevenzione di incendi naturali. L'importanza di tali risultanze a fini probatori nel processo penale però riguarderà un'altra pubblicazione.

4. La segnalazione in caso di violazione del sistema. Prospettive future.

di Tiziana Santoro

Nell'ampio novero delle Pubbliche Amministrazioni ve ne sono alcune che si trovano a dover gestire molteplici banche dati[24], il che si traduce nella possibilità di venire a conoscenza di un'infinità di informazioni, tra cui anche i dati cd. sensibili[25]. Tale opportunità necessita del corrispettivo onere di prestare adeguata protezione a tali dati onde non incorrere nell'accidentale

[24] Appare opportuno fare qualche breve cenno alla nozione giuridica di banca dati. Una prima definizione di banca dati viene data dalla Direttiva 96/9/CE che la definisce "una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo" (art. 1. n. 2) e prevede una tutela giuridica delle "banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore" (art. 3). La tutela delle banche dati in base al diritto di autore non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto: ciò significa che la tutela in parola è accordata non al suo contenuto bensì ai criteri che sono alla base del suo funzionamento: ad es. modalità di accesso e di ricerca, che devono essere più di uno. La titolarità della b.d. spetta "all'autore di una b.d., la persona fisica o il gruppo di persone fisiche che l'ha creata o, qualora la legislazione dello Stato membro interessato lo consenta, la persona giuridica individuata da tale legislazione come titolare del diritto". L'accesso ad una b.d., ad opera dell'utente legittimo gli consente di compiere una serie di operazioni, quali la riproduzione, la traduzione, la distribuzione al pubblico, la comunicazione, ecc. che gli sono necessarie per l'accesso al contenuto della b.d. e l'impiego normale di quest'ultima senza l'autorizzazione dell'autore della b.d. (art. 5). In ambito nazionale troviamo una prima definizione di b.d. nella c.d. legge madre sulla privacy, L 675/96, abrogata e sostituita dal decreto legislativo n. 196/2003, recante il "Codice in materia di protezione dei dati personali", che all'art. 4, lett. p, primo comma, recita: "p) 'banca di dati', qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti." Il D.lgs. 169/99 recante "Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati", definisce "le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto." La normativa in materia di trattamento dei dati personali fa riferimento alla nozione di archivio di dato personale mentre la seconda focalizza l'attenzione sul fronte della tutela giuridica delle b.d. Accanto alla categoria rappresentata dalle b.d. private si collocano le b.d. pubbliche che sono quelle facenti capo alle pubbliche amministrazioni individuate attraverso l'art. 1 del Decreto Legislativo n. 165/2001. La scriminante tra le due categorie è costituita dalle finalità che sottendono la creazione e la gestione della b.d. che nel caso in questione deve corrispondere a finalità pubbliche, ovvero al soddisfacimento dell'interesse pubblico. La Legge n. 340 del 2000 (Legge di semplificazione 1999), contiene un esplicito riferimento alle b.d. pubbliche e l'art. 25 prende in considerazione due distinti aspetti: il primo relativo alla titolarità dei programmi, per cui "1. Le pubbliche amministrazioni (…) che siano titolari di programmi applicativi realizzabili su specifiche indicazioni del committente pubblico, hanno facoltà di darli in uso gratuito ad altre amministrazioni pubbliche, che li adattano alle proprie esigenze"; il secondo riguardante il diritto di accesso alle b.d. da parte delle singole pubbliche amministrazioni che "hanno accesso gratuito ai dati contenuti in pubblici registri, elenchi, atti o documenti da chiunque conoscibili".

[25] All'interno dei dati personali, i dati sensibili sono quelli che rivelano l'origine razziale ed etnica, le convinzioni filosofiche e religiose, le opinioni politiche, le adesioni a partiti od organizzazioni, i dati genetici e biometrici, lo stato di salute, la vita e l'orientamento sessuale del singolo individuo. Il trattamento dei dati sensibili è possibile solo se c'è il consenso esplicito dell'interessato. Il consenso deve essere esplicito e specifico, cioè dato per specifiche finalità di trattamento. In assenza di consenso, i dati possono essere trattati solo nei casi previsti dall'art 9 lett. b) -j) GDPR.

perdita degli stessi o, peggio, nell'ipotesi di possibile furto di dati a causa di accessi inappropriati interni o esterni.

Prima dell'avvento del web, quando la quasi totalità degli archivi era ancora cartacea, il sistema di protezione dei dati era rudimentale: semplicemente, ci si avvaleva di diverse piattaforme, non comunicanti tra di loro, per memorizzare i dati, i quali venivano in un secondo momento trasposti su supporti fisici (*floppy disk*) che venivano conservati in archivi posti anche a grande distanza dal luogo in cui l'informazione era stata immagazzinata.

Ciò permetteva di tenere in luogo sicuro i dati anche in caso di calamità (*disaster recovery plan* della Pubblica Amministrazione) per poterli recuperare in un secondo momento, anche se il lato negativo era dato dalla scomodità di dover trasportare fisicamente i supporti da un posto all'altro, il che non è certo sinonimo di immediatezza della consultazione.

Poi c'è stata un'evoluzione: gli enormi processori e le vecchie piattaforme sono stati sostituiti via via dagli emulatori, cioè software che fanno finta di essere quelli più vecchi ma che possono essere utilizzati dai sistemi operativi recenti.

Si è poi arrivati, con l'avvento del web, alla intranet: un ambiente virtuale in cui possono interagire solo coloro che sono autorizzati a farlo (per esempio, chi lavora in una stessa amministrazione o azienda).

La intranet è un ambiente di lavoro protetto da incursioni esterne, in quanto per entrare è necessario munirsi di apposite credenziali che vengono rilasciate dalla stessa amministrazione proprietaria della rete su cui si opera o, se non direttamente dall'amministrazione, da società dalla stessa autorizzate.

È necessario quindi autenticarsi per poter accedere: l'autenticazione avviene tramite una combinazione di nome utente + password, o numero di matricola + password.

La intranet però prevede anche la possibilità per i terzi di accedere per periodi limitati e per finalità specifiche, quali quelle di porre quesiti alla pubblica amministrazione autenticandosi con il proprio *spid* (identità digitale). Ciò è possibile perchè un accesso alla intranet fatto da un utente e non da un operatore non solo è tracciato dalla chiave digitale con cui si accede, ma può avvenire solo per il fine specifico di interagire a livello di scambio di informazioni: non è possibile a questo livello per il terzo estraneo accedere anche agli archivi di produzione del dato. Solo l'utente eventualmente abilitato alla gestione potrebbe effettuare modifiche sui dati (per esempio, entro nella

mia area personale del sito delle Poste per cambiare il numero di telefono collegato al mio account).

Quindi, gli accessi esterni sono permessi solo quando sono autorizzati e quando non sono finalizzati alla modifica dei data base.

Come fa la Pubblica Amministrazione a controllare e a prevenire accessi abusivi?

Il controllo avviene su due fronti: uno esterno ed uno interno.

Per quanto riguarda il lato interno, il controllo viene svolto dagli uffici preposti alla sicurezza informatica che si trovano presso le sedi centrali delle Amministrazioni oppure anche presso società esterne. All'intero di questi uffici ogni informatico ha un suo compito specifico, c'è chi controlla la rete, chi gli accessi, chi i dati di navigazione, in maniera tale da avere la mappatura in tempo reale di tutto quanto avviene sui dispositivi dell'ufficio e sui *laptop* in dotazione al personale. Qualora il funzionario, anche solo per disattenzione, dovesse prodursi in attività di tipo sospetto, scatterebbe un *alert* in tempo reale direttamente presso l'ufficio centrale. Qui gli informatici avviserebbero della situazione l'informatico preposto alla sede territoriale presso cui si trova il funzionario attenzionato, in maniera tale che possa più facilmente verificare sul posto cosa stia succedendo contattando direttamente il funzionario e verificando l'*hash* dei file presenti sul singolo pc. L'impronta *hash* è un particolare tipo di impronta informatica (cioè una sequenza di lettere e cifre che identificano in modo univoco un file o un documento) generata utilizzando la funzione di *hash*, ovvero un tipo di algoritmo non invertibile. La verifica di questi file permette di individuare il tipo di attività che si stava compiendo e la sua eventuale pericolosità.

Il pericolo però può arrivare anche da un operatore esterno che si trovi ad interagire con la intranet senza essere un operatore autorizzato: un tale soggetto potrebbe creare danni al sistema delle banche dati?

Il problema della *cybersecurity* delle pubbliche amministrazioni è sempre molto sentito e periodicamente sale alla ribalta della cronaca in caso di episodi di fragilità del sistema, come successe nel 2019 in seguito al "caso Exodus", un software spia nascosto tra le normali *app* scaricabili da Google Play Store utilizzato da Polizia e Procure italiane per le sole intercettazioni di reati di criminalità organizzata e terrorismo che, a causa di un bug nei sistemi operativi Android, ha invece permesso di monitorare in modo illecito i dati di centinaia di utenti estranei a qualsiasi procedimento penale. O nel 2021, quando un attacco hacker esterno ai danni della Regione Lazio ha visto il

sabotaggio del CED, dei sistemi informatici, del portale Salute e della rete preposta alla prenotazione dei vaccini della Regione.

La situazione attuale per ciò che riguarda le misure di sicurezza ICT per le pubbliche amministrazioni è indicata nel Piano triennale per l'informatica nella Pubblica Amministrazione[26] (di cui è stata pubblicata l'edizione aggiornata 2024-2026), in cui sono contenute le direttive per favorire la trasformazione digitale del Paese e le linee guida per la sicurezza informatica della p.a.

Il Piano propone di favorire uno sviluppo etico, sostenibile ed inclusivo grazie alla digitalizzazione e all'innovazione, che deve avere come presupposto fondamentale la sicurezza dei dati, al fine di ottenere la fiducia nei servizi erogati e nelle piattaforme istituzionali.

Le misure minime per la *cybersecurity* nelle istituzioni e nella Pubblica Amministrazione sono quindi raccolte nel piano triennale ICT e sono atte a creare un livello di sicurezza coerente per tutti i portali digitali di accesso ai servizi pubblici. Le misure minime sono un importante supporto metodologico, utile soprattutto alle Amministrazioni più piccole, che hanno meno possibilità di avvalersi di professionalità specifiche, e che grazie a questo strumento possono verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento. Le misure minime hanno il merito di fornire un riferimento operativo direttamente utilizzabile (*checklist*), stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili, forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento, responsabilizzando le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.

Una buona idea potrebbe essere quella, già in uso presso alcune Amministrazioni, di utilizzare il sistema *blockchain*, che è un sistema di concentramento delle informazioni che permette di capire se l'informazione su cui si sta lavorando è effettivamente autentica, sia nella forma che nel contenuto. La tecnologia *blockchain* è un meccanismo di database avanzato che permette la condivisione trasparente di informazioni all'interno di una rete aziendale. Un database *blockchain* archivia i dati in blocchi collegati tra loro in una catena. I dati sono cronologicamente coerenti perché non è possibile eliminare o modificare la catena senza il consenso della rete. Il punto di forza di questo sistema consiste nel fatto che una modifica fatta dal singolo deve essere certificata da più server per poter essere accettata. Pertanto, un utente

[26] https://www.agid.gov.it/it/agenzia/piano-triennale

esterno che si inserisse in un data base con l'intento di modificare o distruggere i dati ivi contenuti non potrebbe farlo perchè non potrebbe operare modifiche in solitaria senza che gli altri blocchi della catena approvino.

Il nuovo Piano 2024-2026 si inserisce nel più ampio contesto di riferimento definito dal programma strategico "Decennio Digitale 2030", istituito dalla Decisione (UE) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, i cui obiettivi sono articolati in quattro dimensioni: competenze digitali, servizi pubblici digitali, digitalizzazione delle imprese e infrastrutture digitali sicure e sostenibili, ed è concepito, tra gli altri punti, anche per la sicurezza e la protezione dei dati personali (*data protection by design e by default*)[27].

Il Piano infatti ha introdotto già nel 2021 la strategia *Cloud Italia*, il cui intento è quello di arrivare alla migrazione dei dati e degli applicativi informatici verso un ambiente *cloud* sicuro accessibile alle Pubbliche Amministrazioni, in linea con i principi di tutela della privacy e con le raccomandazioni delle istituzioni europee e nazionali. I vantaggi di questa strategia sono molteplici: si va dall'ammodernamento della p.a. alla diminuzione del rischio di *lock-in* con le aziende fornitrici di software, ridurre significativamente i costi di manutenzione di centri elaborazione dati (data center) obsoleti e delle applicazioni *legacy*, valorizzando al contempo le infrastrutture digitali del Paese più all'avanguardia che stanno attuando il percorso di adeguamento rispetto ai requisiti del Regolamento AGID e relativi atti successivi dell'Agenzia per la Cybersicurezza Nazionale e incrementare la sicurezza delle infrastrutture pubbliche contro possibili cyber attacchi.

L'approdo futuro di questa strategia potrebbe essere quello della creazione del *cloud federato*, in cui più Amministrazioni stipuleranno tra loro accordi volti alla realizzazione di infrastrutture *cloud* federate della p.a. per raggiungere maggiori livelli di affidabilità, sicurezza ed elasticità, purché siano rispettati i princìpi di efficacia ed efficienza dell'azione amministrativa e della normativa applicabile.

Gli attributi chiave di un siffatto modello *cloud* dovrebbero essere, in sintesi:

- sicurezza intrinseca – integrata da zero, che garantisce il massimo livello di sicurezza richiesto all'interno del quadro normativo;
- interoperabilità, reversibilità, portabilità – la possibilità di migrare tra diverse soluzioni *cloud* private e pubbliche senza soluzione di

[27] https://www.agid.gov.it/it/agenzia/piano-triennale

continuità in base alle esigenze di consumo del *cloud*, senza rischi e senza costi nascosti;

- *open-source based* – la possibilità di impiegare diverse soluzioni tecnologiche, basate sull'open-source o proprietarie, per evitare la dipendenza da soluzioni proprietarie e *lock-in*;
- *cloud Neutral* – la possibilità di eseguire la migrazione dei carichi di lavoro da una soluzione *cloud* a un'altra, riportare il carico di lavoro nel punto originario o gestire carichi di lavoro su servizi *cloud* diversi contemporaneamente;
- sostenibile – i miglioramenti nelle tecnologie green sono fondamentali per raggiungere l'obiettivo della Commissione Europea di garantire che i data center siano *carbon-neutral* entro il 2030 – attraverso il controllo dei carichi di lavoro, l'automazione e la riduzione delle apparecchiature hardware ad alta intensità energetica[28].

Si pensi, per fare un esempio concreto, all'ANPR, l'Anagrafe Nazionale che raccoglie tutti i dati anagrafici dei cittadini residenti in Italia e dei cittadini italiani residenti all'estero, aggiornata con continuità dagli oltre 7900 Comuni italiani, consentendo di avere un set di dati anagrafici dei cittadini certo, accessibile, affidabile e sicuro su cui sviluppare servizi integrati ed evoluti per semplificare e velocizzare le procedure tra Pubbliche Amministrazioni e con il cittadino. Sul portale ANPR, nell'area riservata del cittadino, sono attualmente disponibili i servizi che consentono al cittadino di visualizzare i propri dati anagrafici; effettuare una richiesta di rettifica per errori materiali; richiedere autocertificazioni precompilate con i dati anagrafici presenti in ANPR; richiedere un certificato anagrafico in bollo o in esenzione (sono disponibili 15 tipologie differenti di certificati); comunicare un cambio di residenza; visualizzare il proprio domicilio digitale, costantemente allineato con l'Indice Nazionale dei Domicili Digitali (INAD); comunicare un punto di contatto (mail o telefono).

Al fine di agevolare lo sviluppo di sistemi integrati ed evoluti, che semplifichino e velocizzino le procedure tra le Pubbliche Amministrazioni, ANPR ha reso disponibili 28 e-service sulla Piattaforma Nazionale Digitale Dati (PDND) - Interoperabilità, consentendo la consultazione dei dati ANPR da parte di altri Enti aventi diritto, nel rispetto dei principi del Regolamento Privacy.

[28]Sono questi i contenuti del piano ITC dell'Inps, in linea con quello individuato dal Piano Triennale della PA per la trasformazione digitale del Paese che prevede macro-ambiti di intervento relativi ai datacenter, alla modernizzazione applicativa e al cloud, alla connettività, all'interoperabilità, alle piattaforme e ai dati della PA, alla sicurezza, agli ecosistemi, all'accesso ai servizi e alla governance.

ANPR si sta integrando con le anagrafi settoriali del lavoro, della pensione e del welfare e ogni nuova anagrafe che abbia come riferimento la popolazione residente sarà logicamente integrata con ANPR.

In questa ottica, l'obiettivo futuro potrebbe essere quello di creare un unico punto di accesso nazionale dedicato al Welfare, lo Sportello Unico Digitale del Welfare, che potrebbe vedere la cooperazione tra gli Enti del welfare, Enti Locali e altre pp.aa. per realizzare un *common data hub* (dove confluiscono informazioni sulle prestazioni erogate in tema di welfare su tutto il territorio nazionale), e uno sportello unico digitale per accogliere le richieste di prestazione (veicolandole poi all'erogatore effettivo) a prescindere dal soggetto erogatore e facilitare quindi le domande (maggiore standardizzazione, possibilità di raggruppare più domande) e le verifiche (grazie alle banche dati condivise), con tempi di erogazione più veloci e maggiore efficacia.

Il tutto, anche in ossequio del principio del "*once only*" che non permette alla p.a. di richiedere al cittadino informazioni già in suo possesso: un'unica piattaforma interattiva tra p.a. permetterebbe di avere a disposizione in qualunque momento tutti i dati necessari per erogare le prestazioni al cittadino in maniera sicura e veloce.

Ci si chiede se questo basti per impedire violazioni esterne al sistema come gli attacchi degli hacker.

In realtà, l'unico vero modo per porsi al riparo da queste situazioni è, attualmente, quello di investire sulla sicurezza del sistema informatico, in particolare aggiornando costantemente gli antivirus. Le Pubbliche Amministrazioni più importanti, infatti, collaborano attivamente con le aziende che producono gli antivirus per mantenersi sempre protette.

Altre accortezze devono essere tenute dagli operatoti autorizzati per evitare che qualcuno utilizzi fraudolentemente le credenziali autorizzate, quindi cambiare spesso le password, custodire le credenziali in luoghi sicuri, non lasciare il pc aperto e incustodito, fare sempre il *logout* una volta chiusa la sessione di lavoro, ecc. Sono questi, infatti, i modi più frequenti in cui può verificarsi l'intrusione dall'esterno: il caso classico è la mail infettata da un *malware* contenuto in un allegato che viene ingenuamente aperta su un pc di servizio. Anche in un caso simile, però, un'attenta gestione della sicurezza informatica permette di limitare di molto i danni: una rete ben protetta permette di gestire il *malware* lasciandolo confinato nel singolo pc senza permettergli di attaccare la rete condivisa dal pc stesso.